明 細 書

鍵配信システム

技術分野

[0001] 本発明は、複数の受信装置に共有鍵を配信する鍵配信システムに関し、特に、共有鍵を取得するために必要な情報を受信装置毎に個別にすることで、もし受信装置に割り当てられている情報が漏洩しても、その漏洩元の受信装置を追跡可能な技術に関する。

背景技術

[0002] ADSLや光ファイバーなどに代表される高速通信路の普及に伴い、デジタル化された音楽や映像等のコンテンツを通信路を介して提供するサービスが盛んに行われるようになった。このようなサービスの普及に伴い、不正コピーなどに代表されるコンテンツ不正利用を防止する著作権保護方式が必要となってきている。一般に、このコンテンツ不正利用を防止する著作権保護方式には、暗号技術が用いられる。つまり、あるコンテンツ暗号化鍵を用いてデジタルコンテンツを暗号化して通信路を介して配布し、そのコンテンツ暗号化鍵に対応するコンテンツ復号化鍵を与えられている受信装置のみが、暗号化されたコンテンツを復号化して、元のデジタルコンテンツの再生を行うことが出来るというものである。

[0003] ところで、通常、受信装置に与えられているコンテンツ復号化鍵は秘密に保持されるが、装置の不正解析などによって、攻撃者が全受信装置共通に与えられているコンテンツ復号化鍵を取得する可能性がある。ある受信装置に与えられているコンテンツ復号化鍵が一旦漏洩してしまうと、攻撃者はこの漏洩元の追跡が不可能なコンテンツ復号化鍵を用いてデジタルコンテンツの復号化を行う不正な受信装置を作成し、コンテンツの不正利用を行うおそれがある。そのようなコンテンツ不正利用を防ぐ手段の一つとして、受信装置毎に個別の鍵を持たせることによって、漏洩元の受信装置の追跡を可能にするシステムが考えられる。全受信装置に同じデータを送るような放送局型のコンテンツ配信において、コンテンツ不正利用を防止する方式としては、例えば下記非特許文献1に記載された鍵配信システムがある。

[0004] 図53は、非特許文献1に記載された従来の鍵配信システムを示すものである。図53において、通信路90は、後述する鍵発行センタ91及びサーバ92及び複数の受信装置93a一93nを接続している通信路であり、インターネットや放送網等のネットワークで実現されている。また、鍵発行センタ91と複数の受信装置93a一93nの全ての組は、予め一つの個別鍵IKa・・・IKnを共有しており、例えば鍵発行センタ91と受信装置93aは個別鍵IKaを、鍵発行センタ91と受信装置93bは個別鍵IKbを、鍵発行センタ91と受信装置93nは個別鍵IKnを予め共有しているとする。

[0005] まず、全ての受信装置93a一93nで共通中間鍵SMKを共有する方法について説明する。鍵発行センタ91は、共通中間鍵SMKを作成し、その共通中間鍵SMKをサーバ92に送信する。次に、それぞれの受信装置93a一93nと予め共有している個別鍵IKa、IKb, ・・・IKnに基づき、その共通中間鍵SMKを暗号化し、その各暗号文Enc(IKa, SMK)、Enc(IKb, SMK)、・・・、Enc(IKn、SMK)を結合した値を暗号化共通中間鍵群ENCSMKG＝Enc(IKa、SMK)｜｜Enc(IKb, SMK)｜｜・・・Enc(IKn, SMK)として複数の受信装置93a一93nへ向けて配信する。ここで、"｜｜"は結合記号であり、Enc(K, P)は暗号化鍵Kを用いて平文Pを暗号化した際の暗号文を意味する。なお、非特許文献1においては、暗号化共通中間鍵群ENCSMKGのことを個別情報(EMM)、個別鍵IKa一IKnのことをマスター鍵(Km)、共通中間鍵SMKのことをワーク鍵(Kw)とそれぞれ呼んでいる。暗号化共通中間鍵群ENCSMKGを受信した複数の受信装置93a一93nは、暗号化共通中間鍵群ENCSMKGの中から自身の持つ個別鍵に対応する暗号文を抜き出し、個別鍵に基づきその暗号文の復号化を行い、共通中間鍵SMKを取得する。こうすることによって、全受信装置93a一93nで共通の共通中間鍵SMKを共有することが出来る。

[0006] 次に、全ての受信装置93a一93nで、例えばコンテンツ等を復号化する際に用いる共有鍵SKを共有する方法について説明する。サーバ92は、共有鍵SKを作成し、受信装置93a一93nと共有している共通中間鍵SMKに基づき、その共有鍵SKを暗号化し、その暗号文Enc(SMK, SK)を暗号化共有鍵ENCSKとして複数の受信装置93a一93nへ向けて配信する。暗号化共有鍵ENCSKを受信した複数の受信装置93a一93nは、共通中間鍵SMKに基づき暗号化共有鍵ENCSKの復号化を行

い、共有鍵SKを取得する。こうすることによって、全受信装置93aー93nで共通の共有鍵SKを共有することが出来る。なお、非特許文献1においては、共有鍵SKのことをスクランブル鍵(Ks)、暗号化共通鍵ENCSKのことを共有情報(ECM)とそれぞれ呼んでいる。なお、サーバ92が新たな共有鍵SKを基に暗号化共有鍵ENCSKを生成し、その暗号化共有鍵ENCSKを複数の受信装置93aー93nへ配信することによって、新たな共有鍵SKへ更新することも出来る。

[0007] なお、鍵発行センタ91は、共通中間鍵SMKを更新することによって、ある特定の個別鍵を有する受信装置を無効化し、共有鍵SKを取得出来ないようにすることも出来る。ここでは、受信装置93aの個別鍵を有する受信装置を無効化する場合について説明する。まず、共通中間鍵SMKを新たに作成し、その共通中間鍵SMKをサーバ92に送信する。その後、受信装置93aと予め共有している個別鍵IKaを除く全ての個別鍵IKbーIKnのそれぞれを用いて、その共通中間鍵SMKの暗号化を行い、その各暗号文Enc(IKb, SMK)、・・・、Enc(IKn、SMK)を結合した値を暗号化共通中間鍵群ENCSMKG=Enc(IKb, SMK)||・・・Enc(IKn、SMK)として複数の受信装置93aー93nへ配信する。そうすることにより、受信装置93a以外の受信装置93bー93nでは共通中間鍵SMKを取得出来るため、共有鍵SKが得られるが、受信装置93aでは、共通中間鍵SMKを取得出来ないため、共有鍵SKが得られなくなる。このようにすることによって、鍵発行センタ91は、受信装置を無効化することが出来る。なお、受信装置93a以外の受信装置93bー93nを無効化する場合も、受信装置93aの場合と同様の動作となるが、共通中間鍵SMKを暗号化する際に用いる個別鍵が変わる点が異なる。

[0008] このようなシステムにより、もし攻撃者によって、受信装置93aー93nのうちの何れかの受信装置に埋め込まれている個別鍵が不正に取得され、攻撃者がその個別鍵を用いた受信装置を作ったとしても、その受信装置に埋め込まれている個別鍵から漏洩元の受信装置を追跡することが出来るため、対象受信装置の無効化などの対策を打つことが可能となる。

非特許文献1:「デジタル放送局システムのしくみ」 映像情報メディア学会 編 オーム出版局

非特許文献2:「現代暗号理論」 池野信一、小山謙二共著 電子情報通信学会 編

非特許文献3:「THE ART OF COMPUTER PROGRAMMING Vol. 2 ー SEMINUMERICAL ALGORITHMS」 DONALD E. KNUTH 著 ISBN 0−201−03822−6

発明の開示

発明が解決しようとする課題

[0009] 受信装置93aー93nのうちの何れかの受信装置に埋め込まれている個別鍵が不正に取得された場合に、先で述べた方法の他に、攻撃者がその個別鍵を用いて共通中間鍵SMKを取得し、その共通中間鍵SMKを埋め込んだ不正な受信装置を作る場合が考えられる。そのような攻撃に対して、先に述べた従来の構成では、共通中間鍵SMKは全ての受信装置93aー93nで共通の値であったため、その不正な受信装置に埋め込まれている鍵(共通中間鍵SMK)から漏洩元の受信装置を追跡することが出来ないという課題を有していた。

[0010] 本発明は、上記課題を解決するもので、攻撃者によって中間鍵を埋め込んだ不正な受信装置が作成されたとしても、漏洩元の受信装置を追跡することが可能な鍵配信システムを提供することを目的とする。

課題を解決するための手段

[0011] 請求項1における発明は、共有鍵を配信する鍵配信システムであって、前記鍵配信システムは、前記共有鍵を基に共通情報を生成し、前記共通情報を配信するサーバと、前記共通情報及び個別中間鍵群集合を基に、前記共有鍵を取得する複数の受信装置と、から構成され、前記受信装置は、一以上のシステム秘密変数群に基づく一以上の個別中間鍵からなる個別中間鍵群を複数含む前記個別中間鍵群集合を少なくとも異なる二種類以上含む複数の前記個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、前記サーバと前記受信装置のそれぞれは通信路を介して通信可能であって、前記サーバは、前記共有鍵を格納する共有鍵格納部と、予め与えられた一以上の前記システム秘密変数群からなるシステム秘密変数群集合を格納するシステム秘密変数群格納部と、前記共有鍵を基に、前記共通情報を生成する複数の共通情報生成部と、複数の前記共通情報生成部

の中から一つを選択する共通情報生成部選択部と、前記共通情報を複数の前記受信装置に同時に、または、個別に配信する共通情報配信部と、を備え、前記複数の共通情報生成部は、各々、共通情報生成方法が異なり、前記共通情報生成方法を使用して、前記システム秘密変数群集合及び前記共有鍵に基づき、鍵更新データを作成し、前記共通情報生成方法に対応付けられた共通情報識別子及び前記鍵更新データを含む前記共通情報を生成し、前記受信装置は、前記共通情報を受信する共通情報受信部と、複数の共通情報生成方法の各々に対応する前記個別中間鍵群からなる前記個別中間鍵群集合を格納する個別中間鍵群格納部と、複数の前記共通情報生成部に対応する複数の共有鍵取得部と、複数の前記共有鍵取得部の中から一つを選択する共有鍵取得部選択部と、を備え、前記共有鍵取得部選択部は、前記共通情報受信部で受信した前記共通情報に含まれる前記共通情報識別子に基づき、前記複数の共有鍵取得部の中から一つを選択し、前記共有鍵取得部は、前記共通情報識別子に対応した共有鍵取得方法と前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とする。

[0012] 請求項2における発明は、請求項1に記載の鍵配信システムであって、複数の前記共通情報生成方法は、第一共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記サーバには、一以上の時変変数生成式及び一以上のサーバ共通中間鍵生成式が予め与えられており、前記受信装置のそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、前記第一共通情報生成方法は、一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一システム秘密変数群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成し、前記鍵更新データは、前記時変変

数群及び前記暗号化共有鍵を含む、方法であり、前記第一共有鍵取得方法は、前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0013] 請求項3における発明は、請求項1に記載の鍵配信システムであって、前記サーバには、前記複数の個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、前記サーバは、予め与えられた前記個別中間鍵群集合を格納する個別中間鍵群集合格納部と、を備え、複数の前記共通情報生成方法は、第一共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記サーバには、一以上の時変変数生成式及び一以上の受信装置共通中間鍵生成式が予め与えられており、前記受信装置のそれぞれには、前記受信装置共通中間鍵生成式が予め与えられており、前記第一共通情報生成方法は、一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一個別中間鍵群及び前記時変変数群及び前記受信装置共通中間鍵生成式を基に、共通中間鍵を生成し、前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成し、前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含む、方法であり、前記第一共有鍵取得方法は、前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0014] 請求項4における発明は、請求項1記載の鍵配信システムであって、複数の前記共通情報生成方法は、第二共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第二共通情報生成方法と対となる第二共有鍵取得方法を含み、前記システ

ム秘密変数群集合は、複数の第二システム秘密鍵から成る第二システム秘密鍵群を含み、前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、前記第二共通情報生成方法は、前記第二システム秘密鍵群に含まれる一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生成し、前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成し、前記鍵更新データは、前記暗号化共有鍵群を含む、方法であり、前記第二共有鍵取得方法は、前記鍵更新データに含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする。

[0015] 請求項5における発明は、請求項4に記載の鍵配信システムであって、前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含み、前記第二共通情報生成方法は、前記第二システム秘密鍵群に含まれる複数の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生成し、前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成する方法であることを特徴とする。

[0016] 請求項6における発明は、請求項1記載の鍵配信システムであって、前記鍵配信システムは、さらに、前記通信路を介して前記受信装置のそれぞれに接続され、個別情報群を配信する鍵発行センタと、を備え、前記鍵発行センタは、予め前記受信装置に与えられた一以上の個別鍵を格納する出力装置対応情報格納部と、前記個別情報を生成する複数の個別情報生成部と、前記個別情報及び前記個別情報生成部に対応付けられた個別情報識別子の組を二種類以上含む前記個別情報群を、複数の前記受信装置に同時に、または、個別に配信する個別情報群配信部と、を備え、前記個別情報生成部は、各々、個別情報生成方法が異なり、前記個別情報生成方法を基に、前記個別情報識別子及び前記システム秘密変数群及び前記個別情報を出力し、前記受信装置は、予め与えられた前記個別鍵を格納する個別鍵格納部と、前記個別情報群を受信する個別情報群受信部と、複数の前記個別情報生成部に

対応する複数の個別中間鍵群取得部と、を備え、前記個別情報受信部は、受信した前記個別情報群に含まれる前記個別情報識別子に基づき、複数の前記個別中間鍵群取得部のそれぞれへ、前記個別情報識別子に対応する前記個別情報を出力し、前記個別中間鍵取得部は、前記個別情報識別子に対応した個別中間鍵取得方法を使用して、前記個別情報及び前記個別鍵に基づき、前記個別中間鍵群を取得することを特徴とする。

[0017] 請求項7における発明は、請求項6に記載の鍵配信システムであって、前記複数の個別情報生成部は、さらに、前記システム秘密変数群を生成し、前記鍵発行センタは、前記システム秘密変数群及び前記個別情報生成部に対応付けられた前記個別情報識別子の組を二種類以上含む前記システム秘密変数群集合を前記サーバへ配布するシステム秘密変数群集合送信部と、を備え、前記サーバは、配布された前記システム秘密変数群集合を前記システム秘密変数群格納部へ格納するシステム秘密変数群集合受信部と、を備えることを特徴とする。

[0018] 請求項8における発明は、請求項6記載の鍵配信システムであって、前記鍵発行センタは、前記通信路を介して前記サーバに接続され、前記システム秘密変数群集合送信部は、前記通信路を介して前記サーバへ前記システム秘密変数群集合を配信し、前記システム秘密変数群集合受信部は、前記通信路を介して前記鍵発行センタから前記システム秘密変数群集合を受信することを特徴とする。

[0019] 請求項9における発明は、請求項6記載の鍵配信システムであって、前記システム秘密変数群集合送信部は、可搬媒体へ前記システム秘密変数群集合を記録し、前記システム秘密変数群集合受信部は、前記可搬媒体に記録された前記システム秘密変数群集合を読み取ることを特徴とする。

[0020] 請求項10における発明は、請求項7記載の鍵配信システムであって、前記鍵発行センタと前記サーバは、予めサーバ鍵を共有しているとし、前記システム秘密変数群集合送信部は、前記サーバ鍵を基に前記システム秘密変数群集合を暗号化して、暗号化データを作成して、前記サーバへ配布し、前記システム秘密変数群集合受信部は、配布された前記暗号化データを前記サーバ鍵を基に復号化し、前記システム秘密変数群集合を取得することを特徴とする。

[0021] 請求項11における発明は、請求項6記載の鍵配信システムであって、複数の前記個別情報生成方法は、第一個別情報生成方法を含み、複数の前記個別中間鍵取得方法は、前記第一個別情報生成方法と対となる第一個別中間鍵群取得方法を含み、前記鍵発行センタは、予め与えられる期間鍵及び前記期間鍵に対応付けられた前記第一システム秘密変数群及び前記期間鍵に対応付けられた期間識別子の組を一種類以上格納する期間情報格納部と、を備え、前記受信装置の前記個別鍵格納部のそれぞれは、前記期間鍵を基に、前記第一個別中間鍵群が暗号化されることにより生成された暗号化第一個別中間鍵群及び前記期間鍵に対応付けられた前記期間識別子の組を一種類以上格納しており、前記第一個別情報生成方法は、前記期間情報格納部の中から、一組の前記期間鍵及び前記第一システム秘密変数群及び前記期間識別子を選択し、各々の前記個別鍵を基に、前記期間鍵を暗号化し、複数の暗号化期間鍵を生成し、前記個別情報群は、前記複数の暗号化期間鍵を結合した暗号化期間鍵群及び前記期間識別子からなる第一個別情報を含み、前記第一個別中間鍵群取得方法は、前記個別鍵に基づき、前記第一個別情報に含まれる前記複数の暗号化期間鍵のいずれか一つの前記暗号化期間鍵を復号化し、前記期間鍵を取得し、前記個別鍵格納部に含まれる一以上の前記暗号化第一個別中間鍵群の中から、前記期間識別子に対応付けられた前記暗号化第一個別中間鍵群を一つ選択し、前記期間鍵に基づき、前記暗号化第一個別中間鍵群を復号化することによって、前記第一個別中間鍵群を取得する方法であることを特徴とする。

[0022] 請求項12における発明は、請求項6記載の鍵配信システムであって、複数の前記個別情報生成方法は、第二個別情報生成方法を含み、複数の前記個別中間鍵取得方法は、前記第二個別情報生成方法と対となる第二個別中間鍵群取得方法を含み、前記第二個別情報生成方法は、各々の前記個別鍵に対して、複数の前記第二システム秘密鍵のいずれか一つを選定し、各々の前記個別鍵に基づき、選定した前記第二システム秘密鍵を暗号化し、複数の暗号化第二システム秘密鍵を生成し、前記個別情報群は、前記複数の暗号化第二システム秘密鍵を結合した暗号化第二システム秘密鍵群を含む第二個別情報を含み、前記第二個別中間鍵群取得方法は、前記第二個別情報に含まれる前記複数の暗号化第二システム秘密鍵の中から、前

記個別鍵に対応する前記暗号化第二システム秘密鍵を一つ選定し、前記個別鍵に基づき、選定した前記暗号化第二システム秘密鍵を復号化することによって、前記第二システム秘密鍵を取得し、その前記第二システム秘密鍵を前記第二個別中間鍵群とする方法であることを特徴とする。

[0023] 請求項13における発明は、請求項2記載の鍵配信システムであって、前記個別中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0024] 請求項14における発明は、請求項2記載の鍵配信システムであって、前記時変変数生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0025] 請求項15における発明は、請求項2記載の鍵配信システムであって、前記サーバ共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0026] 請求項16における発明は、請求項2記載の鍵配信システムであって、前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0027] 請求項17における発明は、請求項4記載の鍵配信システムであって、前記第二システム秘密鍵群は、10個の第二システム秘密鍵から成ることを特徴とする。

[0028] 請求項18における発明は、共有鍵を配信するサーバと、前記共有鍵を受信する複数の受信装置と、を備える鍵配信システムにおける受信装置であって、前記受信装置は、外部から共通情報を受信する共通情報受信部と、複数の共有鍵取得方法の各々に対応する個別中間鍵群から成る個別中間鍵群集合を格納する個別中間鍵群格納部と、複数の前記共有鍵取得方法に対応する複数の共有鍵取得部と、複数の前記共有鍵取得部の中から一つを選択する共有鍵取得部選択部と、を備え、前記共有鍵取得部選択部は、前記共通情報受信部で受信した前記共通情報に含まれる共通情報識別子に基づき、前記共有鍵取得部を一つ選択し、前記共有鍵取得部は、前記共通情報識別子に対応した前記共有鍵取得方法及び前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とする。

[0029] 請求項19における発明は、請求項18に記載の受信装置であり、複数の前記共有鍵取得方法は、第一共有鍵取得方法を含み、前記個別中間鍵群集合は、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記受信装置のそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、前記共通情報は、時変変数群及び暗号化共有鍵からなる第一共通情報を含み、前記第一共有鍵取得方法は、前記第一共通情報に含まれる前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0030] 請求項20における発明は、請求項18記載の受信装置であって、複数の前記共有鍵取得方法は、第二共有鍵取得方法を含み、前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、前記共通情報は、前記複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵を暗号化することで生成された一以上の暗号化共有鍵を含む暗号化共有鍵群からなる第二共通情報を含み、前記第二共有鍵取得方法は、前記共通第二共通情報に含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする。

[0031] 請求項21における発明は、請求項20記載の受信装置であって、前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする。

[0032] 請求項22における発明は、請求項18記載の受信装置であって、前記鍵配信システムは、さらに、前記通信路を介して前記受信装置のそれぞれとサーバに接続され、個別情報群を配信する鍵発行センタと、を備え、前記受信装置は、予め与えられた個別鍵を格納する個別鍵格納部と、外部から前記個別情報群を受信する個別情報群受信部と、複数の個別中間鍵取得方法に対応する複数の個別中間鍵群取得部と

、を備え、前記個別情報受信部は、受信した前記個別情報群に含まれる個別情報識別子に基づき、複数の前記個別中間鍵群取得部のそれぞれへ、前記個別情報群に含まれ前記個別情報識別子に対応する前記個別情報を出力し、前記個別中間鍵取得部は、前記個別情報識別子に対応した前記個別中間鍵取得方法を使用して、前記個別情報及び前記個別鍵に基づき、前記個別中間鍵群を取得することを特徴とする。

[0033] 請求項23における発明は、請求項19記載の受信装置であって、複数の前記個別中間鍵取得方法は、第一個別中間鍵群取得方法を含み、前記受信装置の前記個別鍵格納部のそれぞれは、期間鍵を基に、第一個別中間鍵群を暗号化することにより生成される暗号化第一個別中間鍵群及び前記期間鍵に対応付けられた期間識別子の組を一種類以上格納しており、前記個別情報群は、それぞれの前記個別鍵を基に前記期間鍵を暗号化して生成された複数の暗号化期間鍵を含む暗号化期間鍵群及び前記期間識別子からなる第一個別情報を含み、前記第一個別中間鍵群取得方法は、前記個別鍵に基づき、前記第一個別情報に含まれる前記複数の暗号化期間鍵のいずれか一つの前記暗号化期間鍵を復号化し、前記期間鍵を取得し、前記個別鍵格納部に含まれる一以上の前記暗号化第一個別中間鍵群の中から、前記期間識別子に対応付けられた前記暗号化第一個別中間鍵群を一つ選択し、前記期間鍵に基づき、前記暗号化第一個別中間鍵群を復号化することによって、前記第一個別中間鍵群を取得する方法であることを特徴とする。

[0034] 請求項24における発明は、請求項20記載の受信装置であって、複数の前記個別中間鍵取得方法は、第二個別中間鍵群取得方法を含み、前記個別情報群は、それぞれの前記個別鍵を基に、前記第二システム秘密鍵のいずれかを暗号化することによって生成された複数の暗号化第二システム秘密鍵からなる暗号化第二システム秘密鍵群を含む第二個別情報を含み、前記第二個別中間鍵群取得方法は、前記第二個別情報に含まれる前記複数の暗号化第二システム秘密鍵の中から、前記個別鍵に対応する前記暗号化第二システム秘密鍵を一つ選定し、前記個別鍵に基づき、選定した前記暗号化第二システム秘密鍵を復号化することによって、前記第二システム秘密鍵を取得し、その前記第二システム秘密鍵を前記第二個別中間鍵群とする

方法であることを特徴とする。

[0035] 請求項25における発明は、請求項19記載の受信装置であって、前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0036] 請求項26における発明は、共有鍵を配信するサーバと、通信路を介して接続され、前記共有鍵を受信する処理をコンピュータに実行させるプログラムであって、外部から共通情報を受信するステップと、複数の共有鍵取得方法の各々に対応する個別中間鍵群から成る個別中間鍵群集合を格納するステップと、複数の前記共有鍵取得方法に対応する複数の共有鍵取得ステップと、前記共通情報受信部で受信した前記共通情報に含まれる共通情報識別子に基づき、前記共有鍵取得部を一つ選択するステップと、をコンピュータに実行させ、前記共有鍵取得ステップは、前記共通情報識別子に対応した前記共有鍵取得方法及び前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とする。

[0037] 請求項27における発明は、請求項26記載のプログラムであって、複数の前記共有鍵取得方法は、第一共有鍵取得方法を含み、前記個別中間鍵群集合は、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記プログラムのそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、前記共通情報は、時変変数群及び共通中間鍵を基に前記共有鍵を暗号化することにより生成される暗号化共有鍵からなる第一共通情報を含み、前記第一共有鍵取得方法は、前記第一共通情報に含まれる時変変数群、及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0038] 請求項28における発明は、請求項26記載のプログラムであって、複数の前記共有鍵取得方法は、第二共有鍵取得方法を含み、前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、前記共通情報は、前記複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵を基に前記共有鍵を暗号化することにより生成され

る複数の暗号化共有鍵からなる暗号化共有鍵群を含む第二共通情報を含み、前記第二共有鍵取得方法は、前記共通第二共通情報に含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする。

[0039] 請求項29における発明は、請求項28記載のプログラムであって、前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする。

[0040] 請求項30における発明は、請求項27記載のプログラムであって、前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする。

[0041] 請求項31における発明は、請求項26記載のプログラムを記録した媒体であることを特徴とする。

[0042] 請求項32における発明は、共有鍵を配信する鍵配信方法であって、前記鍵配信方法は、前記共有鍵を基に共通情報を生成し、前記共通情報を配信する鍵配信ステップと、前記共通情報及び個別中間鍵群集合を基に、前記共有鍵を取得する複数の鍵受信ステップと、から構成され、前記鍵受信ステップには、一以上のシステム秘密変数群に基づく一以上の個別中間鍵からなる個別中間鍵群を複数含む前記個別中間鍵群集合を少なくとも異なる二種類以上含む複数の前記個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、前記鍵配信ステップは、前記共有鍵を格納するステップと、予め与えられた一以上のシステム秘密変数群からなるシステム秘密変数群集合を格納するステップと、前記共有鍵を基に、前記共通情報を生成する複数の共通情報生成ステップと、複数の前記共通情報生成ステップの中から一つを選択するステップと、前記共通情報を複数の前記受信装置に同時に、または、個別に配信するステップと、を含み、前記複数の共通情報生成ステップは、各々、共通情報生成方法が異なり、前記共通情報生成方法を使用して、前記システム秘密変数群集合及び前記共有鍵に基づき、鍵更新データを作成

し、前記共通情報生成方法に対応付けられた共通情報識別子及び前記鍵更新データを含む前記共通情報を生成し、前記鍵受信ステップは、前記共通情報を受信するステップと、複数の共通情報生成方法の各々に対応する前記個別中間鍵群からなる前記個別中間鍵群集合を格納するステップと、複数の前記共通情報生成部に対応する複数の共有鍵取得ステップと、前記共通情報受信部で受信した前記共通情報に含まれる前記共通情報識別子に基づき、複数の前記共有鍵取得ステップの中から一つを選択するステップと、を含み、前記共有鍵取得ステップは、前記共通情報識別子に対応した共有鍵取得方法と前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とする。

[0043] 請求項33における発明は、請求項32に記載の鍵配信方法であって、複数の前記共通情報生成方法は、第一共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記鍵配信ステップには、一以上の時変変数生成式及び一以上のサーバ共通中間鍵生成式が予め与えられており、前記鍵受信ステップのそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、前記第一共通情報生成方法は、一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一システム秘密変数群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成する方法であり、前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含み、前記第一共有鍵取得方法は、前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0044] 請求項34における発明は、請求項33に記載の鍵配信方法であって、前記鍵配信

ステップは、前記複数の前記個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、前記鍵受信ステップは、予め与えられた前記個別中間鍵群集合を格納するステップと、を含み、複数の前記共通情報生成方法は、第一共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、前記サーバには、一以上の時変変数生成式及び一以上の共通中間鍵生成式が予め与えられており、前記鍵受信ステップのそれぞれには、前記共通中間鍵生成式が予め与えられており、前記第一共通情報生成方法は、一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一個別中間鍵群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成する方法であり、前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含み、前記第一共有鍵取得方法は、前記時変変数群及び前記第一個別中間鍵群及び前記共通中間鍵生成式を基に、前記共通中間鍵を生成し、前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする。

[0045] 請求項35における発明は、請求項32記載の鍵配信方法であって、複数の前記共通情報生成方法は、第二共通情報生成方法を含み、複数の前記共有鍵取得方法は、前記第二共通情報生成方法と対となる第二共有鍵取得方法を含み、前記システム秘密変数群集合は、複数の第二システム秘密鍵から成る第二システム秘密鍵群を含み、前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、前記第二共通情報生成方法は、前記第二システム秘密鍵群に含まれる一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生

成し、前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成する方法であり、前記鍵更新データは、前記暗号化共有鍵群を含み、前記第二共有鍵取得方法は、前記鍵更新データに含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする。

[0046] 請求項36における発明は、請求項35記載の鍵配信方法であって、前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする。

発明の効果

[0047] 本発明の鍵配信システムによれば、攻撃者によって、受信装置に埋め込まれている個別鍵を不正取得され、その個別鍵を基に得られる中間鍵を埋め込んだ不正な受信装置が作成されたとしても、その中間鍵には、どの個別鍵から生成されたかを示す情報を含んでいるため、不正な受信装置に埋め込まれている中間鍵を調査することによって、漏洩元の受信装置を追跡することが可能となる。

[0048] また、その中間鍵は複数の個別中間鍵から構成されるようにしたので、万が一、いずれかの個別中間鍵の個別情報が偽造されたとしても、残りの個別中間鍵を用いて、漏洩元の受信装置が特定出来るようになったため、追跡可能性が増し、安全性が向上する。

[0049] 以下本発明に係る鍵配信システムの実施の形態について、図面を参照しながら説明する。

図面の簡単な説明

[0050] [図1]本発明の実施の形態1における鍵配信システム1の概要図

[図2]本発明の実施の形態1における鍵発行センタ11の構成例を示す図

[図3]本発明の実施の形態1における第一個別情報生成部112の構成例を示す図

[図4]本発明の実施の形態1における期間情報格納部1122の構成例を示す図

[図5]本発明の実施の形態1における第一システム秘密変数群SPGI__1の一例を示す図

[図6]本発明の実施の形態1における第一個別情報EMMIの一例を示す図

[図7]本発明の実施の形態1における受信装置対応情報格納部113の構成例を示す図

[図8]本発明の実施の形態1における第二個別情報生成部114の構成例を示す図

[図9]本発明の実施の形態1における第二システム秘密変数群SPGIIの一例を示す図

[図10]本発明の実施の形態1における第二個別中間鍵群MKIIGaの一例を示す図

[図11]本発明の実施の形態1における第二個別情報EMMIIの一例を示す図

[図12]本発明の実施の形態1におけるシステム秘密変数群集合SPGSの一例を示す図

[図13]本発明の実施の形態1における個別情報群EMMGの一例を示す図

[図14]本発明の実施の形態1における鍵発行センタ11の鍵情報配信時の処理の流れ図

[図15]本発明の実施の形態1における鍵発行センタ11の第一システム秘密変数群SPGI及び第一個別情報EMMI生成時の処理の流れ図

[図16]本発明の実施の形態1における鍵発行センタ11の第二システム秘密変数群SPGII及び第二個別情報EMMII生成時の処理の流れ図

[図17]本発明の実施の形態1におけるサーバ12の構成例を示す図

[図18]本発明の実施の形態1におけるシステム秘密変数群格納部122の構成例を示す図

[図19]本発明の実施の形態1における第一共通情報生成部125の構成例を示す図

[図20]本発明の実施の形態1における時変変数群PRGの一例を示す図

[図21]本発明の実施の形態1における第一共通情報ECMIの一例を示す図

[図22]本発明の実施の形態1における第二共通情報生成部126の構成例を示す図

[図23]本発明の実施の形態1における暗号化共有鍵群ENCSKGの一例を示す図

[図24]本発明の実施の形態1における第二共通情報ECMIIの一例を示す図

[図25]本発明の実施の形態1におけるサーバ12のシステム秘密変数群集合SPGSを受信した時の処理の流れ図

[図26]本発明の実施の形態1におけるサーバ12の共有鍵SK更新時の処理の流れ図

[図27]本発明の実施の形態1における受信装置13aの構成例を示す図

[図28]本発明の実施の形態1における個別鍵格納部1304aの構成例を示す図

[図29]本発明の実施の形態1における暗号化第一個別中間鍵群集合ENCMKIGSaの一例を示す図

[図30]本発明の実施の形態1における第一個別中間鍵群MKIGaの一例を示す図

[図31]本発明の実施の形態1における個別中間鍵格納部1305aの構成例を示す図

[図32]本発明の実施の形態1における受信装置13aの鍵発行センタ11から個別情報群EMMGを受信した時の処理の流れ図

[図33]本発明の実施の形態1における受信装置13aのサーバ12から共通情報ECMを受信した時の処理の流れ図

[図34]本発明の実施の形態2における鍵配信システム2の概要図

[図35]本発明の実施の形態2における鍵発行センタ21の構成例を示す図

[図36]本発明の実施の形態2における第三個別情報生成部212の構成例を示す図

[図37]本発明の実施の形態2における第三システム秘密変数群集合SPGIIISの一例を示す図

[図38]本発明の実施の形態2における第三個別情報EMMIIIの一例を示す図

[図39]本発明の実施の形態2における鍵発行センタ21の鍵情報配信時の処理の流れ図

[図40]本発明の実施の形態2における鍵発行センタ21の第三システム秘密変数群集合SPGIIIS及び第三個別情報EMMIII生成時の処理の流れ図

[図41]本発明の実施の形態2におけるサーバ22の構成例を示す図

[図42]本発明の実施の形態2におけるシステム秘密変数群格納部222の構成例を示す図

[図43]本発明の実施の形態2における第三共通情報ECMIIIの一例を示す図

[図44]本発明の実施の形態2におけるサーバ22の第三システム秘密変数群集合SPGIIISを受信した時の処理の流れ図

[図45]本発明の実施の形態2におけるサーバ22の共有鍵SK更新時の処理の流れ図

[図46]本発明の実施の形態2における受信装置23aの構成例を示す図

[図47]本発明の実施の形態2における個別鍵格納部2304aの構成例を示す図

[図48]本発明の実施の形態2における個別中間鍵格納部2305aの構成例を示す図

[図49]本発明の実施の形態2における受信装置23aの鍵発行センタ21から第三個別情報群EMMIIIを受信した時の処理の流れ図

[図50]本発明の実施の形態2における受信装置23aのサーバ22から第三共通情報ECMIIIを受信した時の処理の流れ図

[図51]本発明の実施の形態1における鍵配信システム1の変形例

[図52]本発明の実施の形態1における第一共通情報生成部125の変形例

[図53]従来の鍵配信システムの概要図

符号の説明

[0051] 10 通信路

11、21 鍵発行センタ

12、22 サーバ

13a一13n、23a一23n 受信装置

111、211 第一制御部

112 第一個別情報生成部

212 第三個別情報生成部

1121 期間選択部

2121 第三システム秘密変数群生成部

1122 期間情報格納部

2122 第一中間鍵群生成部

1123 期間鍵暗号化部

113 受信装置対応情報格納部

114 第二個別情報生成部

1141 第二システム秘密鍵生成部

1142 第二個別中間鍵群暗号化部

115 システム秘密変数群集合送信部

215 第三システム秘密変数群集合送信部

116 個別情報群配信部

216 第三個別情報配信部

121、221 システム秘密変数群集合受信部

122、222 システム秘密変数群格納部

123 共有鍵生成部

124 共通情報生成部選択部

125 第一共通情報生成部

225 第三共通情報生成部

1251 時変変数群生成部

1252 共通中間鍵取得部

1253 第一共有鍵暗号化部

1254 第二制御部

126 第二共通情報生成部

1261 第二共有鍵暗号化部

1262 第三制御部

127、227 共通情報配信部

1301、2301 個別情報群受信部

1302a 第一個別中間鍵群取得部

2302a 第三個別中間鍵群取得部

1303a 第二個別中間鍵群取得部

1304a、2304a 個別鍵格納部

1305a、2305a 個別中間鍵群格納部

1306、2306a 共通情報受信部

1307a 共有鍵取得部選択部

1308a 第一共有鍵取得部

2308a 第三共有鍵取得部

1309a 第二共有鍵取得部

1310 出力部

発明を実施するための最良の形態

[0052] (実施の形態1)

本発明に係る一つの実施の形態としての鍵配信システム1について説明する。最初に、図1を用いて本実施形態の概要を説明する。

[0053] 図1において、通信路10は、後述する鍵発行センタ11とサーバ12と複数の受信装置13a一13nとが接続されている通信路であり、インターネットや放送網などのネットワークで実現されている。鍵発行センタ11は共有鍵SKを受信装置へ配信するのに必要な情報であるシステム秘密変数群集合SPGSをサーバ12へ、共有鍵SKを取得するために必要な個別情報群EMMGを複数の受信装置13a一13nへ配信する。サーバ12は、共有鍵SK及びシステム秘密変数群集合SPGSを基に生成された共通情報ECMを複数の受信装置13a一13nへ配信する。複数の受信装置13a一13nは、個別情報群EMMG及び共通情報ECMを基に、共通鍵SKを取得し、その共通鍵SKを外部へ出力する。ここで、鍵発行センタ11と受信装置13a一13nの全ての組には、予め各組が共有している一つの個別鍵が与えられているとし、例えば鍵発行センタ11と受信装置13aは個別鍵IKaを、鍵発行センタ11と受信装置13bは個別鍵IKbを、・・・、鍵発行センタ11と受信装置13nは個別鍵IKnを予め共有しているとする。

[0054] ここでは、各構成要素の動作についてもう少し詳細に説明する。まず、各受信装置13a一13nへ、各々異なる第一個別中間鍵群MKIGa一MKGIn及び第二個別中間鍵群MKIIGa一MKIIGnを配布する方法について説明する。初めに、鍵発行センタ11は、システム秘密変数群集合SPGSを生成し、そのシステム秘密変数群集合SPGSをサーバ12へ向けて送信する。また、第一個別中間鍵群MKIGa一MKIGn及び第二個別中間鍵群MKIIGa一MKIIGn及び個別鍵IKa一IKnを基に、受信装置が第一個別中間鍵群及び第二個別中間鍵群を取得するために必要な個別情報群EMMGを生成し、複数の受信装置13a一13nへ配信する。個別情報群EMMGを

受信した受信装置13aは、予め与えられている個別鍵IKaを用いて、受信装置13aに対応付けられた第一個別中間鍵群MKIGa及び第二個別中間鍵群MKIIGaを取得する。受信装置13a以外の受信装置13bー13nの場合も同様に、各受信装置が持つ個別鍵を用いて、各受信装置に対応付けられた第一個別中間鍵群及び第二個別中間鍵群を取得する。このようにして、各受信装置13aー13nが各々異なる第一個別中間鍵群MKIGaーMKIGn及び第二個別中間鍵群MKIIGaーMKIIGnを保持することが出来る。

[0055] 次に、サーバ12が共有鍵SKを更新する場合の動作について説明する。まず、サーバ12は、予め与えられた条件に従って、システム秘密変数群集合SPGSを基に、第一共通情報ECMIもしくは第二共通情報ECMIIのいずれかを生成し、その第一共通情報ECMIもしくは第二共通情報ECMII及びそのどちらかかを識別する共通情報識別子を含む共通情報ECMとして複数の受信装置13aー13nへ向けて配信する。複数の受信装置13aー13nは、共通情報ECMを受信し、その共通情報ECMに含まれる共通情報識別子を基に、共通情報ECMに含まれているのが第一共通情報ECMIか第二共通情報ECMIIかを判断する。それが第一共通情報ECMIの場合、第一個別中間鍵群と第一共通情報ECMIを用いて、共有鍵SKを取得する。一方、第二共通情報ECMIIの場合、第二個別中間鍵群と第二共通情報ECMIIを用いて、共有鍵SKを取得する。このようにして、受信装置13aー13nの共有鍵SKを更新する。

[0056] なお、本実施形態である鍵配信システム1では、鍵発行センタ11がある特定の個別鍵を持つ受信装置を無効化し、共有鍵SKを取得出来ないようにすることも可能となる。これは、鍵発行センタ11において、システム秘密変数群集合SPGS及び第一個別中間鍵群及び第二個別中間鍵群を更新する際に、無効化したい受信装置に対しては第一個別中間鍵群及び第二個別中間鍵群を取得出来ないように、無効化したい受信装置の保持する個別鍵を用いないようにすることで実現可能である。

[0057] 以上が、本実施形態の概要である。以下に、本発明の鍵配信システムの一実施形態である鍵配信システム1の詳細について説明を行う。これらの構成要素について詳細に説明する。

[0058] ＜鍵配信システム1の構成＞

鍵配信システム1は、図1に示すように、通信路10と、鍵発行センタ11と、サーバ12と、複数の受信装置13a－13nから構成される。

[0059] 鍵発行センタ11は共有鍵SKを受信装置13a－13nへ配信するのに必要な情報であるシステム秘密変数群集合SPGSをサーバ12へ、サーバ12から共有鍵SKを受信するのに必要な個別情報群EMMGを複数の受信装置13a－13nへ配信する。サーバ12は、共有鍵SKを生成し、その共有鍵SK及びシステム秘密変数群集合SPGSを基に共通情報ECMを生成し、その共通情報ECMを複数の受信装置13a－13nへ配信する。受信装置13a－13nは、個別情報群EMMG及び共通情報ECMを基に、共有鍵SKを取得し、外部へ出力する。

[0060] 以下に、これらの構成要素について詳細に説明する。まず、通信路10の構成について述べ、続いて鍵発行センタ11及びサーバ12及び受信装置13a－13nの構成と動作について図を用いて説明する。

[0061] ＜通信路10の構成＞

通信路は、例えば、インターネット、電話回線、専用線、放送網等のようなネットワークである。

[0062] ＜鍵発行センタ11の構成＞

鍵発行センタ11は、図2に示すように、第一制御部111、第一個別情報生成部112、受信装置対応情報格納部113、第二個別情報生成部114、システム秘密変数群集合送信部115、個別情報群配信部116、から構成される。

[0063] (1)第一制御部111

第一制御部111は、予め与えられる個別情報更新条件を満たした場合、もしくは、鍵発行センタ13が動作開始した場合、第一個別情報生成要求REQEMMIを第一個別情報生成部112へ出力し、第二個別情報生成要求REQEMMIIを第二個別情報生成部114へ出力する。例えば、個別情報更新条件は"ある一定期間毎(例:1日、1年)"や"外部からある信号を受信した場合"などがあり、個別情報更新条件が"ある一定期間毎(例:1日、1年)"の場合、第一制御部111がカウンタなどを備えるなどにより実現可能であり、個別情報更新条件が"外部からある信号を受信した場合"の場合、第一制御部111が外部信号を受信する受信部を備えるなどにより実現可能で

ある。

[0064] (2)第一個別情報生成部112

第一個別情報生成部112は、図3に示すように、期間選択部1121と、期間情報格納部1122と、期間鍵暗号化部1123と、から構成される。

[0065] (2−1)期間選択部1121

期間選択部1121は、第一制御部111から第一個別情報生成要求REQEMMIを受信した場合、図4で示すような、未使用フラグ(FLAG__1ーFLAG__k)、期間識別子(PID__1ーPID__k)及び期間鍵(PK__1ーPK__k)及び第一システム秘密変数群(SPGI__1ーSPGIーk)のk組{(FLAG__1、PID__1, PK__1, SPGI__1)、(FLAG__2、PID__2, PK__2, SPGI__2)、・・・、(FLAG__k、PID__k, PK__k, SPGI__k)}を格納している期間情報格納部1122にアクセスする。そして、そのk組の中から、未使用フラグが"1"のものを1組を選択する。そして、選択した組の未使用フラグを"0"に設定する。未使用フラグが"1"のものの中から1組を選択する方法としては、例えば、乱数を用いてランダムに1組を選択する方法などがある。乱数を生成する方法については、非特許文献3が詳しい。以後、期間選択部1121で選択された組のそれぞれの値を、未使用フラグFLAG__i、期間識別子PID__i、期間鍵PK__i、第一システム秘密変数群SPGI__iとする。ここで、未使用フラグFLAG__iは未使用フラグFLAG__1ーFLAG__kのいずれかであり、期間識別子PID__iは期間識別子PID__1ーPID__kのいずれかであり、期間鍵PK__iは期間鍵PK__1ーPK__kのいずれかであり、第一システム秘密変数群SPGI__iは第一システム秘密変数群SPGI__1ーSPGI__kのいずれかであるとする。次に、選択された第一システム秘密変数群SPGI__iを、第一システム秘密変数群SPGIとしてシステム秘密変数群集合送信部115へ出力する。そして、最後に、選択された期間識別子PID__i及び期間鍵PK__iを期間鍵暗号化部1123へ出力する。

[0066] (2−2)期間情報格納部1122

期間情報格納部1122は、図4で示すように、予め与えられる、未使用フラグ及び期間識別子及び期間鍵及び第一システム秘密変数群のk組{(FLAG__1、PID__1, PK__1, SPGI__1)、(FLAG__2、PID__2, PK__2, SPGI__2)、・・・、(FLAG__

k、PID__k, PK__k, SPGI__k)}を格納しているものである。例えば、図4においては、期間識別子PID__1に対応して、期間鍵PK__1及び第一システム秘密変数群SPGI__1及び未使用フラグFLAG__1を保持し、期間識別子PID__2に対応して、期間鍵PK__2及び第一システム秘密変数群SPGI__2及び未使用フラグFLAG__2を保持し、期間識別子PID__kに対応して、期間鍵PK__k及び第一システム秘密変数群SPGI__k及び未使用フラグFLAG__kを保持している状態を表している。ここで、第一システム秘密変数群SPGI__1は、図5のように、5つの第一システム秘密変数(s__1、t__1、u__1、v__1、c__1)から構成されており、また、他の第一システム秘密変数群SPGI__2ーSPGI__kも、それぞれ5つの第一システム秘密変数(s__2、t__2、u__2、v__2、c__2ーs__k、t__k、u__k、v__k、c__k)から構成されている。さらに、第一システム秘密変数は、予め第一システム秘密変数生成式"s__1＊t__1＝u__1＊v__1 mod N"、"s__2＊t__2＝u__2＊v__2 mod N"、・・・、"s__k＊t__k＝u__k＊v__k mod N"を満たすように与えられているものとする。例えば、5つの第一システム秘密変数及びモジュラスNは、例えば128ビットの自然数であり、ここでのモジュラスNの値は、後述する時変変数群生成部1251、共通中間鍵取得部1252、第一共有鍵取得部1308aに予め共通の値として与えられているモジュラスNと同じ値であり、例えば2^{128}などである。また、"mod N"は剰余演算のことであり、"^"はべき乗演算のことであり、例えば2^{4}は16を意味し、以後同じ意味で用いる。なお、第一システム秘密変数群(例:SPGI__1)の作成方法としては、4つの第一システム秘密変数(例:s__1、t__1、u__1、c__1)を乱数として生成し、そのうち3つの第一システム秘密変数(例:s__1、t__1、u__1)を第一システム秘密変数生成式"s__1＊t__1＝u__1＊v__1 mod N"に代入することで、残りの一つの第一システム秘密変数(例:v__1)を求める方法などがある。また、未使用フラグFLAG__1ーFLAG__kのそれぞれは、"0"もしくは"1"で構成されており、例えば自然数などである。なお、鍵発行センタ11が動作開始する際には、未使用フラグFLAG__1ーFLAG__kは全て"1"であるとする。また、受信装置識別子AIDaーAIDnは、それぞれの受信装置13aー13n毎に対応づけられたユニークな識別子であり、例えばそれぞれ異なる自然数である。さらに、期間鍵PK__1ーPK__kのそれぞれは、例えば、非特許文献2に

記載のDES暗号方式の鍵などであり、乱数などを用いて作成される。また、期間識別子PID__1ーPID__kはそれぞれ異なる値をとり、例えば、それぞれ異なる自然数などである。

[0067] (2−3)期間鍵暗号化部1123

期間鍵暗号化部1123は、第一システム秘密変数群選択部から期間識別子PID__i及び期間鍵PK__iを受信した場合、受信装置対応情報格納部114にアクセスして、受信装置識別子AIDaーAIDn及び個別鍵IKaーIKnを全て取得する。そして、まず受信装置識別子AIDaに対して、対応している個別鍵IKaに基づいて期間鍵PK__iの暗号化を行い、その暗号文を暗号化期間鍵ENCPKa＝Enc(IKa, PK__i)とし、受信装置識別子AIDaに対応付ける。そして、他の受信装置識別子AIDbーAIDnに対しても同様に、対応している個別鍵に基づいて期間鍵の暗号化を行い、その暗号文Enc(IKb, PK__i)、・・・、Enc(IKn、PK__i)を暗号化期間鍵ENCPKb、・・・、ENCPKnとし、それぞれの受信装置識別子AIDbーAIDnに対応付ける。そして、図6で示すような、期間識別子PID__i及び装置識別子AIDaーAIDn及び暗号化期間鍵ENCPKaーENCPKnから構成される第一個別情報EMMI＝PID__i||{AIDa, ENCPKa}||{AIDb, ENCPKb}・・・||{AIDn, ENCPKn}}を作成し、その第一個別情報EMMIを、個別情報群配信部116に出力する。ここで期間鍵を暗号化するのに使用する暗号化アルゴリズムは、例えば、非特許文献2に記載のDES暗号方式などであり、後述する受信装置13aー13nの第一個別中間鍵群取得部1302aで暗号化期間鍵を復号化する際に用いる復号化アルゴリズムと同じ方式を用いる。

[0068] (3)受信装置対応情報格納部113

受信装置対応情報格納部113は、図7で示すように、複数の受信装置13aー13nを識別する受信装置識別子AIDaーAIDnと、その各受信装置13aー13nに予め与えられている個別鍵IKaーIKnを格納するものである。例えば、図7においては、受信装置識別子AIDaに対応づけられている受信装置13aは個別鍵IKaを保持し、受信装置識別子AIDbに対応づけられている受信装置13bは個別鍵IKbを保持し、受信装置識別子AIDnに対応づけられている受信装置13nは個別鍵IKnを保持してい

る状態を表している。受信装置対応情報格納部113へは、第一個別情報生成部112内の期間鍵暗号化部1123及び第二個別情報生成部114内の第二個別中間鍵群暗号化部1142からアクセス可能である。

[0069] (4)第二個別情報生成部114

第二個別情報生成部114は、図8に示すように、第二システム秘密鍵生成部1141と、第二個別中間鍵群暗号化部1142と、から構成される。

[0070] (4−1)第二システム秘密鍵生成部1141

第二システム秘密鍵生成部1141は、第一制御部111から第二個別情報生成要求REQEMMIIを受信した場合、6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6を生成する。6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6を生成する方法としては、例えば、ランダムに生成する方法などがあり、具体的には、例えば乱数を用いることにより実現出来る。乱数を生成する方法については、非特許文献3が詳しい。そして、図9で示すような、6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6から成る第二システム秘密変数群SPGIIを作成し、システム秘密変数群集合送信部115及び第二個別中間鍵群暗号化部1142へ出力する。

[0071] (4−2)第二個別中間鍵群暗号化部1142

第二個別中間鍵群暗号化部1142は、第二システム秘密鍵生成部1141から第二システム秘密変数群SPGIIを受信した場合、受信装置対応情報格納部113にアクセスして、受信装置識別子AIDaーAIDn及び個別鍵IKaーIKnを全て取得する。そして、まず受信装置識別子AIDaに対して、第二システム秘密変数群SPGIIに含まれる6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6の中から1つの秘密第二鍵を選択する。この1つの第二システム秘密鍵の選択方法は、例えば、ランダムに選択する方法などがあり、これは乱数を用いることによって実現出来る。ここでは、例として、受信装置識別子AIDaに対して選択した鍵を、第二システム秘密鍵k1とすると、図10で示すように、第二個別中間鍵群MKIIGaは第二システム秘密鍵k1となる。そして、対応している個別鍵IKaに基づいて第二個別中間鍵群MKIIGaの暗号化を行い、その暗号文を暗号化第二個別中間鍵群ENCMKIIGa＝Enc(IKa, MKIIGa)とし、受信装置識別子AIDaに対応付ける。そして、他の受信装置識別子AIDbーAIDn

に対しても同様に、第二システム秘密変数群SPGIIの中の6つの第二システム秘密鍵の中から一つの第二システム秘密鍵を選択し、その第二システム秘密鍵を第二個別中間鍵群とし、対応している個別鍵に基づいて第二個別中間鍵群の暗号化を行い、その暗号文Enc(IKb, MKIIGb)、・・・、Enc(IKn、MKIIGn)を暗号化第二個別中間鍵群ENCMKIIGb、・・・、ENCMKIIGnとし、それぞれの受信装置識別子AIDbーAIDnに対応付ける。そして、図11で示すような、受信装置識別子AIDaーAIDn及び暗号化第二個別中間鍵群ENCMKIIGaーENCMKIIGnから構成される第二個別情報EMMII={AIDa, ENCMKIIGa}||{AIDb, ENCMKIIGb}・・・||{AIDn, ENCMKIIGn}}を作成し、その第二個別情報EMMIIを、個別情報群配信部116に出力する。ここで第二個別中間鍵群を暗号化するのに使用する暗号化アルゴリズムは、例えば、非特許文献2に記載のDES暗号方式などであり、後述する受信装置13aー13nの第二個別中間鍵群取得部1303aで暗号化第二個別中間鍵群を復号化する際に用いる復号化アルゴリズムと同じ方式を用いる。

[0072] (5)システム秘密変数群集合送信部115

システム秘密変数群集合送信部115は、第一個別情報生成部112の第一システム秘密変数群選択部1121から第一システム秘密変数群SPGIを受信し、また、第二個別情報生成部114の第二システム秘密鍵生成部1141から第二システム秘密変数群SPGIIを受信した場合、図12で示すような、第一システム秘密変数群SPGI及びその第一システム秘密変数群SPGIに対応するシステム秘密変数群識別子SPGIDIと、第二システム秘密変数群SPGII及びその第二システム秘密変数群SPGIIに対応するシステム秘密変数群識別子SPGIDIIと、から構成されるシステム秘密変数群集合SPGSを生成する。そして、そのシステム秘密変数群集合SPGSを、サーバ12へ向けて送信する。ここで、システム秘密変数群識別子SPGIDIとシステム秘密変数群識別子SPGIDIIは、例えば、それぞれ異なる自然数である。なお、システム秘密変数群識別子SPGIDIとシステム秘密変数群識別子SPGIDIIは、それぞれ第一システム秘密変数群SPGIと第二システム秘密変数群SPGIIを区別するために用いるが、予め鍵発行センタ11とサーバ12において、送受信データにおける第一システム秘密変数群SPGIと第二システム秘密変数群SPGIIのビット位置などの情報が共有さ

れている場合、システム秘密変数群集合SPGSにおいてシステム秘密変数群識別子SPGIDIとシステム秘密変数群識別子SPGIDIIはなくても良い。

[0073] (6)個別情報群配信部116

個別情報群配信部116は、第一個別情報生成部112の期間鍵暗号化部1123から第一個別情報EMMIを受信し、そして、第二個別情報生成部114の第二個別中間鍵群暗号化部1142から第二個別情報EMMIIを受信した場合、図13で示すような、第一個別情報EMMI及びその第一個別情報EMMIに対応する個別情報識別子EMMIDIと第二個別情報EMMII及びその第二個別情報EMMIIに対応する個別情報識別子EMMIDIIから構成される個別情報群EMMGを生成する。そして、その個別情報群EMMGを、受信装置13a一13nへ向けて配信する。ここで、個別情報識別子EMMIDIと個別情報識別子EMMIDIIは、例えば、それぞれ異なる自然数である。なお、個別情報識別子EMMIDIと個別情報識別子EMMIDIIは、それぞれ第一個別情報EMMIと第二個別情報EMMIIを区別するために用いるが、予め鍵発行センタ11と受信装置13a一13nにおいて、送受信データにおける第一個別情報EMMIと第二個別情報EMMIIのビット位置などの情報が共有されている場合、個別情報群EMMGにおいて個別情報識別子EMMIDIと個別情報識別子EMMIDIIはなくてもよい。

[0074] ＜鍵発行センタ11の動作＞

以上で、鍵発行センタ11の構成について説明を行ったが、ここでは鍵発行センタ11の動作について説明する。ここでは、予め与えられた個別情報更新条件を満たしている場合、もしくは、鍵発行センタ11が動作開始した場合などに、共有鍵を配布、受信するのに必要な鍵情報をサーバ12及び複数の受信装置13a一13nに配信するときの動作について図14に示すフローチャートを用いて説明する。また、第一個別情報生成部112が第一システム秘密変数群SPGI及び第一個別情報EMMIを生成するときの動作の詳細について図15に示すフローチャートを用いて説明する。最後に、第二個別情報生成部114が第二システム秘密変数群SPGII及び第二個別情報EMMIIを生成するときの動作の詳細について図16に示すフローチャートを用いて説明する。

[0075] ≪鍵発行センタ11による鍵情報配信時の動作≫

第一制御部111は、第一個別情報生成部112へ第一個別情報生成要求REQEMMIを出力し、第二個別情報生成部114へ第二個別情報生成要求REQEMMIIを出力する。(S1101)

第一個別情報生成部112は、図15で示すようなフローチャート(下記で詳細を説明)に従って、第一システム秘密変数群SPGI及び第一個別情報EMMIを生成し、第一システム秘密変数群SPGIをシステム秘密変数群集合送信部115へ出力し、第一個別情報EMMIを個別情報群配信部116へ出力する。(S1102)

第二個別情報生成部114は、図16で示すようなフローチャート(下記で詳細を説明)に従って、第二システム秘密変数群SPGII及び第二個別情報EMMIIを生成し、第二システム秘密変数群SPGIIをシステム秘密変数群集合送信部115へ出力し、第二個別情報EMMIIを個別情報群配信部116へ出力する。(S1103)

第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIを受信したシステム秘密変数群集合送信部115は、第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIからなるシステム秘密変数群集合SPGSを生成し、そのシステム秘密変数群集合SPGSをサーバ12へ送信する。(S1104)

第一個別情報EMMI及び第二個別情報EMMIIを受信した個別情報群配信部116は、第一個別情報EMMI及び第二個別情報EMMIIからなる個別情報群EMMGを生成し、その個別情報群EMMGを受信装置13a～13nへ配信し、終了する。(S1105)

≪第一システム秘密変数群SPGI及び第一個別情報EMMIを生成時の動作(ステップS1102の詳細説明)≫

第一個別情報生成要求REQEMMIを受信した第一システム秘密変数群選択部1121は、期間情報格納部1122にアクセスして、未使用フラグが"1"である一組の期間識別子(例:PID__i)と期間鍵(例:PK__i)と第一システム秘密変数群(例:SPGI__i)を取得する。そして、期間選択部1121に格納されている未使用フラグ(例:FLAG__i)を"0"に設定する。(S11021)

第一システム秘密変数群選択部1121は、第一システム秘密変数群(例:SPGI__i

)を第一システム秘密変数群SPGIとしてシステム秘密変数群集合送信部115へ出力する。(S11022)

第一システム秘密変数群選択部1121は、期間識別子(例:PID__i)と期間鍵(例:PK__i)を期間鍵暗号化部1123へ出力する。(S11023)

期間識別子(例:PID__i)と期間鍵(例:PK__i)を受信した期間鍵暗号化部1123は、受信装置対応情報格納部114へアクセスし、受信装置識別子AIDa～AIDn及び個別鍵IKa～IKnの全ての組を取得する。(S11024)

期間鍵暗号化部1123は、それぞれの個別鍵IKa～IKnに基づき、期間鍵(例:PK__i)の暗号化を行い、暗号化期間鍵(例:ENCPKa＝Enc(IKa、PK__i)、・・・、ENCPKn＝Enc(IKn、IKn))を生成する。(S11025)

それぞれの暗号化期間鍵ENCPKa～ENCPKnに暗号化時に使用した個別鍵に対応する受信装置識別子AIDa～AIDnに対応付けて、さらに、期間識別子(例:PID__i)を加えて、第一個別情報EMMI(例:＝PID__i||{AIDa、ENCPKa}||{AIDb、ENCPKb}、・・・、{AIDn、ENCPKn})を生成する。(S11026)

期間鍵暗号化部1123は、第一個別情報EMMIを個別情報群配信部116へ出力して、終了する。(S11027)

≪第二システム秘密変数群SPGII及び第二個別情報EMMIIを生成時の動作(ステップS1103の詳細)≫

第二個別情報生成要求REQEMMIIを受信した第二システム秘密鍵生成部1141は、6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6を生成する。(S11031)

第二第二システム秘密鍵生成部1141は、6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6から成る第二システム秘密変数群SPGIIを生成する。(S11032)

第二システム秘密鍵生成部1141は、第二システム秘密変数群SPGIIをシステム秘密変数群集合送信部115及び第二個別中間鍵群暗号化部1142へ出力する。(S11033)

第二システム秘密変数群SPGIIを受信した第二個別中間鍵群暗号化部1142は、受信装置対応情報格納部113にアクセスして、受信装置識別子AIDa～AIDn及び個別鍵IKa～IKnを全て取得する。(S11034)

第二個別中間鍵群暗号化部1142は、受信装置識別子AIDa～AIDnのそれぞれに対して、第二システム秘密変数群SPGIIの中から1つの第二システム秘密鍵を選択し(例:MKIIGa＝k1、MKIIGb＝k2、・・・、MKIIGn＝k6)、第二個別中間鍵群MKIIGa～MKIIGnとする。(S11035)

第二個別中間鍵群暗号化部1142は、個別鍵IKaに基づいてそれぞれの第二個別中間鍵群MKIIGa～MKIIGnの暗号化を行い、その暗号文を暗号化第二個別中間鍵群ENCMKIIGa＝Enc(IKa, MKIIGa)、ENCMKIIGb＝Enc(IKb、MKIIGb)、・・・、ENCMKIIGn＝Enc(IKn、MKIIGn)とする。(S11036)

第二個別中間鍵群暗号化部1142は、受信装置識別子AIDa～AIDn及び暗号化第二個別中間鍵群ENCMKIIGa～ENCMKIIGnから構成される第二個別情報EMMII＝{AIDa, ENCMKIIGa}||{AIDb, ENCMKIIGb}・・・||{AIDn, ENCMKIIGn}}を作成する。(S11037)。

[0076] 第二個別中間鍵群暗号化部1142は、第二個別情報EMMIIを、個別情報群配信部116に出力する。(S11038)

以上が、鍵配信システム1の構成要素である鍵発行センタ11の構成と動作である。続いて、サーバ12の構成と動作について説明を行う。

[0077] ＜サーバ12の構成＞

サーバ12は、図17に示すように、システム秘密変数群集合受信部121、システム秘密変数群格納部122、共有鍵生成部123、共通情報生成部選択部124、第一共通情報生成部125、第二共通情報生成部126、共通情報配信部127、とから構成される。

[0078] (1)システム秘密変数群集合受信部121

システム秘密変数群集合受信部121が、鍵発行センタ11からシステム秘密変数群集合SPGSを受信した場合、受信したシステム秘密変数群集合SPGSに含まれるシステム秘密変数群識別子であるSPGIDIとSPGIDIIに基づき、第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIを抽出し、図18で示すようなシステム秘密変数群格納122に格納し、共有鍵生成部123へ共有鍵生成要求REQSKを出力する。

[0079] (2)システム秘密変数群格納部122

システム秘密変数群格納部122は、図18で示すように第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIを格納するものである。システム秘密変数群格納部122へは、システム秘密変数群集合受信部121及び第一共通情報生成部125内の時変変数群生成部1251と共通中間鍵取得部1252及び第二共通情報生成部126内の第二共有鍵暗号化部1261からアクセス可能である。

[0080] (3)共有鍵生成部123

共通鍵生成123は、システム秘密変数群集合受信部121から共有鍵生成要求REQSKを受信した場合、もしくは、予め与えられる共通情報更新条件を満たしている場合、共有鍵SKを生成する。共有鍵SKを生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。乱数を生成する方法については、非特許文献3が詳しい。そして、その共有鍵SKを共通情報生成部選択部124へ出力する。例えば、共通情報更新条件が"1秒毎"や"1時間毎"などの場合、共有鍵生成部123がカウンタを備えるなどにより実現可能であり、共通情報更新条件が"外部から特定信号を受信した場合"などの場合、共有鍵生成部123が外部信号を受信する受信部を備えるなどにより実現可能である。

[0081] (4)共通情報生成部選択部124

共通情報生成部選択部124は、共有鍵生成部123から共有鍵SKを受信した場合、第一共通情報生成部125か第二共通情報生成部126のいずれかを選択し、その選択した第一共通情報生成部125の時変変数群生成部1251と第一共有鍵暗号化部1253、もしくは、第二共通情報生成部126の第二共有鍵暗号化部1261へ共有鍵SKを出力する。ここで、第一共通情報生成部125か第二共通情報生成部126のいずれかを選択する方法としては、例えば、外部から与えられるスケジュールデータに基づき選択する方法や、乱数を用いてランダムに選択するなどがある

(5)第一共通情報生成部125

第一共通情報生成部125は、図19に示すように、時変変数群生成部1251と、共通中間鍵取得部1152と、第一共有鍵暗号化部1253と、第二制御部1254と、から構成される。

[0082] (5−1)時変変数群生成部1251

時変変数群生成部1251は、共通情報生成部選択部124から共有鍵SKを受信した場合、4つの乱数z、w、m、nを生成する。ここで、乱数z、w、m、nを生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。また、乱数z、w、m、nは、例えば、それぞれ128ビットの自然数である。また、システム秘密変数群格納部122にアクセスし、第一システム秘密変数群SPGIを取得し、その中から第一システム秘密変数s、t、u、v、とを抽出する。そして、予め与えられる4つの時変変数生成式"r1＝s＊z＋v＊m mod N"、"r2＝t＊w＋u＊n N"、"r3＝u＊z＋t＊m mod N"、"r4＝v＊w＋s＊n N"を基に、4つの時変変数r1、r2、r3、r4を生成する。その後、生成した時変変数r1、r2、r3、r4から構成される、図20で示すような時変変数群PRGを生成し、その時変変数群PRGを第二制御部1254へ出力する。最後に、共通中間鍵取得部1252へ向けて乱数z、w、m、nを出力する。

[0083] (5−2)共通中間鍵取得部1252

共通中間鍵取得部1252は、時変変数群生成部1251から乱数z、w、m、nを受け取った場合、まず、システム秘密変数群格納122にアクセスし、第一システム秘密変数群SPGIを取得し、その中から第一システム秘密変数s、t、u、v、cを抽出する。その後、共通中間鍵SMKを、予め与えられるサーバ共通中間鍵生成式"SMK＝2＊s＊t＊(z＋w＋c＋n＊m)＋2＊(u＊s＊n＊z＋t＊v＊m＊w) mod N"に基づいて生成し、その生成した共通中間鍵SMKを第一共有鍵暗号化部1253へ出力する。

[0084] (5−3)第一共有鍵暗号化部1253

第一共有鍵暗号化部1253は、第二制御部124から共有鍵SKを受信し、さらに、共通中間鍵取得部1252から共通中間鍵SMKを受信した場合、その共通中間鍵SMKに基づいて、受け取った共有鍵SKの暗号化を行う。ここで共有鍵SKの暗号化に使用する暗号化アルゴリズムは、例えば、DES暗号方式などであり、後述する受信装置13a～13nの各第一共有鍵取得部1308aにおいて暗号化共有鍵ENCSKを復号化するのに用いる復号化アルゴリズムと同じ方式を用いる。その後、暗号化共有鍵ENCSKを第二制御部1254に出力する。

[0085] (5−4)第二制御部1254

第二制御部1254は、時変変数群生成部1251から時変変数群PRGを受信し、また、第一共有鍵暗号化部1253から暗号化共有鍵ENCSKを受信した場合、図21で示すように、第一共通情報ECMIであることを示す共通情報識別子ECMIDI及び時変変数群PRG及び暗号化共有鍵ENCSKからなる、第一共通情報ECMIを生成する。そして、その第一共通情報ECMIを共通情報ECMとして、共通情報配信部127へ出力する。ここで、共通情報識別子ECMIDIは、例えば自然数である。なお、共通情報識別子ECMIDIは、共通情報ECMに含まれているデータが第一共通情報ECMIか第二共通情報ECMIIかを区別する際に用いるが、予めサーバ12と受信装置13a−13nにおいて、第一共通情報ECMIと第二共通情報ECMIIを送り出すタイミングを共有している場合、共通情報ECMに第一共通情報識別子ECMIDI及び第二共通情報識別子ECMIDIIがなくても良い。例えば、サーバ12と受信装置13a−13nにおいて、ある決められた時刻では第一共通情報ECMIを送信し、それ以外では第二共通情報ECMIIを送信する場合などである。

[0086] (6)第二共通情報生成部126

第二共通情報生成部126、図22に示すように、第二共有鍵暗号化部1261と、第三制御部1262と、から構成される。

[0087] (6−1)第二共有鍵暗号化部1261

第二共有鍵暗号化部1261は、第二制御部124から共有鍵SKを受信した場合、まず、システム秘密変数群格納122にアクセスし、第二システム秘密変数群SPGIIを取得し、その中から6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6を抽出する。そして、まず第二システム秘密鍵k1を基に、共有鍵SKを暗号化し、暗号化共有鍵ENCSK1＝Enc(k1、SK)を生成する。そして、他の第二システム秘密鍵k2、k3、k4、k5、k6に対しても、同様に、共有鍵SKを暗号化し、暗号化共有鍵ENCSK2＝Enc(k2、SK)、・・・、ENCSK6＝Enc(k6、SK)を生成する。最後に、図23で示すような、暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENCSK6を連結したものを、暗号化共有鍵群ENCSKGとして、第三制御部1262に出力する。なお、ここで共有鍵SKの暗号化に使用する暗号化アルゴリズムは、例えば、

DES暗号方式などであり、後述する受信装置13a－13nの各第二共有鍵取得部1309aにおいて暗号化共有鍵群ENCSKGのいずれかの暗号文を復号化するのに用いる復号化アルゴリズムと同じ方式を用いる。

[0088] (6−2)第三制御部1262

第三制御部1262は、第二共有鍵暗号化部1261から暗号化共有鍵ENCSKGを受信した場合、図24で示すように、第二共通情報ECMIIであることを示す共通情報識別子ECMIDII及び暗号化共有鍵群ENCSKGからなる、第二共通情報ECMIIを生成する。そして、その第二共通情報ECMIIを共通情報ECMとして、共通情報配信部127へ出力する。ここで、共通情報識別子ECMIDIIは、例えば共通情報識別子ECMIDIと異なる自然数である。なお、共通情報識別子ECMIDIIは、共通情報ECMに含まれているデータが第一共通情報ECMIか第二共通情報ECMIIかを区別する際に用いるが、予めサーバ12と受信装置13a－13nにおいて、第一共通情報ECMIと第二共通情報ECMIIを送り出すタイミングを共有している場合、共通情報ECMに第一共通情報識別子ECMIDI及び第二共通情報識別子ECMIDIIがなくても良い。例えば、サーバ12と受信装置13a－13nにおいて、ある決められた時刻では第一共通情報ECMIを送信し、それ以外では第二共通情報ECMIIを送信する場合などである。

[0089] (7)共通情報配信部127

共通情報配信127は、第一共通情報生成部125の第二制御部1254、もしくは、第二共通情報生成部126の第三制御部1262、のいずれかから共通情報ECMを受信した場合、受信装置13a－13nへその共通情報ECMを配信する。

[0090] ＜サーバ12の動作＞

以上で、サーバ12の構成について説明を行ったが、ここでサーバ12の動作について説明する。まず、鍵発行センタ11から共有鍵SKを配信する際に用いるシステム秘密変数群集合SPGSを受信した際の動作について図25に示すフローチャートを用いて説明する。次に、システム秘密変数群集合受信部121から共有鍵生成要求REQSKを受信した場合、もしくは、予め与えられた共有鍵更新条件を満たした場合、サーバ12が受信装置13a－13nへ新たな共有鍵SKを配信する際の動作について図

26に示すフローチャートを用いて説明する。

[0091] ≪鍵発行センタ11からシステム秘密変数群集合SPGSを受信した時の動作≫

システム秘密変数群集合受信部121は、受信したシステム秘密変数群集合SPGSの中に含まれるシステム秘密変数群識別子SPGIDIーSPGIDIIを基に、第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIを抽出する。(S1201)

システム秘密変数群集合受信部121は、第一システム秘密変数群SPGI及び第二システム秘密変数群SPGIIをシステム秘密変数群格納部122へ格納し、終了する。(S1202)

≪サーバ12が受信装置13aー13nへ、新たな共有鍵SKを配信する時の動作≫

共有鍵生成部123は、共有鍵SKを生成し、共通情報生成部選択部124へ出力する。(S1251)

共通情報生成部選択部124は、第一共通情報生成部125か第二共通情報生成部126のどちらかを選択し、選択した方へ共有鍵SKを出力する。ここで、第一共通情報生成部125を選択した場合、ステップS1254へ進む。反対に、第二共通情報生成部126を選択した場合、ステップS1260へ進む。(S1252)

共有鍵情報選択部124から共有鍵SKを受信した第一共通情報生成部125は、乱数z、w、m、nを生成する。その後、システム秘密変数群格納122にアクセスし、第一システム秘密変数群SPGIを取得し、その中から第一システム秘密変数s、t、u、vとを抽出する。そして、予め与えられる4つの時変変数生成式"r1＝s＊z＋v＊m mod N"、"r2＝t＊w＋u＊n N"、"r3＝u＊z＋t＊m mod N"、"r4＝v＊w＋s＊n N"を基に、4つの時変変数r1、r2、r3、r4を生成する。生成した4つの時変変数r1、r2、r3、r4から構成される、時変変数群PRGを生成する。(S1253)

その時変変数群PRGを第二制御部1254へ出力する。(S1254)

共通中間鍵取得部1252に向けて乱数z、w、m、nを出力する。(S1255)

共通中間鍵取得部1252は、時変変数群生成部1251から乱数z、w、m、nを受け取った場合、まず、システム秘密変数群格納122にアクセスし、第一システム秘密変数群SPGIを取得し、その中から第一システム秘密変数s及びt及びu及びv及びcを抽出する。そして、共通中間鍵SMKを、予め与えられるサーバ共通中間鍵生成式"

SMK＝2＊s＊t＊(z＋w＋c＋n＊m)＋2＊(u＊s＊n＊z＋t＊v＊m＊w) mod N"に基づいて取得する。(S1256)

生成した共通中間鍵SMKを第一共有鍵暗号化部1253に出力する。(S1257)

第一共有鍵暗号化部1253は、第二制御部124から共有鍵SKを受信し、さらに、共通中間鍵取得部1252から共通中間鍵SMKを受信した場合、その共通中間鍵SMKに基づいて、受け取った共有鍵SKの暗号化を行い、暗号化共有鍵ENCSKを生成し、その暗号化共有鍵ENCSKを第二制御部1254に出力する。(S1258)

第二制御部1254は、時変変数群生成部1251から時変変数群PRGを受信し、また、第一共有鍵暗号化部1253から暗号化共有鍵ENCSKを受信した場合、第一共通情報ECMIであることを示す共通情報識別子ECMIDI及び時変変数群PRG及び暗号化共有鍵ENCSKからなる、第一共通情報ECMIを生成し、その第一共通情報ECMIを共通情報ECMとして、共通情報配信部127へ出力する。ステップS1264へ進む。(S1259)

第二共有鍵暗号化部1261は、第二制御部124から共有鍵SKを受信した場合、まず、システム秘密変数群格納122にアクセスし、第二システム秘密変数群SPGIIを取得し、その中から6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6を抽出する。(1260)

第二共有鍵暗号化部1261は、それぞれの第二システム秘密鍵k1、k2、k3、k4、k5、k6を基に、共有鍵SKを暗号化し、暗号化共有鍵ENCSK1＝Enc(k1、SK)、ENCSK2＝Enc(k2、SK)、・・・、ENCSK6＝Enc(k6、SK)を生成し、暗号化共有鍵ENCSK1～ENCSK6を連結して、暗号化共有鍵群ENCSKGを生成する。(S1261)

第二共有鍵暗号化部1261は、暗号化共有鍵群ENCSKGを、第三制御部1262に出力する。(S1262)

第三制御部1262は、第二共有鍵暗号化部1261から暗号化共有鍵群ENCSKGを受信した場合、第二共通情報ECMIIであることを示す共通情報識別子ECMIDII及び暗号化共有鍵群ENCSKGからなる、第二共通情報ECMIIを生成し、その第二共通情報ECMIIを共通情報ECMとして、共通情報配信部127へ出力する。(S126

3)

共通情報ECMを受信した共通情報配信部127は、受信装置13aー13nへ共通情報ECMを配信して、終了する。(S1264)

以上が、鍵配信システム1の構成要素であるサーバ12の構成と動作である。続いて、受信装置13aー13nの構成と動作について説明を行う。まず、受信装置13aの構成と動作について説明を行い、次に、受信装置13aと他の受信装置13bー13nとの相違点について述べる。

[0092] ＜受信装置13aの構成＞

受信装置13aは、図27に示すように、個別情報受信部1301、第一個別中間鍵群取得部1302a、第二個別中間鍵群取得部1303a、個別鍵格納部1304a、個別中間鍵格納部1305a、共通情報受信部1306、第二選択部1307a、第一共有鍵取得部1308a、第二共有鍵取得部1309a、出力部1310、とから構成される。ここで、第一個別中間鍵群取得部1302a、第一個別中間鍵群取得部1303a、個別鍵格納部1304a、個別中間鍵格納部1305a、第二選択部1307a、第一共有鍵取得部1308a、第二共有鍵取得部1309a、は受信装置13a固有の構成要素であり、個別情報受信部1301、共通情報受信部1306、出力部1310、は受信装置13aー13nにおいて共通の構成要素である。

[0093] (1)個別情報受信部1301

個別情報受信部1301が、サーバ12から、個別情報群EMMGを受信した場合、受信した個別情報群EMMGの中に含まれる個別情報識別子EMMIDI、EMMIDIIに基づき、第一個別情報EMMI及び第二個別情報EMMIIを抽出し、第一個別情報EMMIを第一個別中間鍵群取得部1302aへ、第二個別情報EMMIIを第二個別中間鍵群取得部1303aへ出力する。

[0094] (2)第一個別中間鍵群取得部1302a

第一個別中間鍵群取得部1302aは、個別情報受信部1301から第一個別情報EMMIを受信した場合、まず図28に示すような個別鍵格納部1304aから受信装置識別子AIDa及び個別鍵IKa及び暗号化第一個別中間鍵群集合ENCMKIGSaを取得する。そして、受信した第一個別情報EMMIから、期間識別子(例えばPID__i:PI

D__iはPID__1ーPID__kのいずれか)、及び、個別鍵格納部1304aに格納されていた受信装置識別子AIDaに対応する暗号化期間鍵ENCPKaを取得する。その後、個別鍵格納部1304に格納されている個別鍵IKaに基づき、暗号化期間鍵ENCPKaの復号化を行い、期間識別子PID__iに対応する期間鍵PK__iを取得する。その後、図29で示すような暗号化第一個別中間鍵群集合ENCMKIGSaの中から、第一個別情報EMMIの中の期間識別子(例:PID__i、PID__iはPID__1ーPID__kのいずれか)に対応する暗号化第一個別中間鍵群(例えばENCMKIGa__i:ENCMKIGa__iはENCMKIGa__1ーENCMKIGa__kのいずれか)を取得し、期間鍵PK__iに基づき、その暗号化第一個別中間鍵群の復号化を行い、図30で示すような第一個別中間鍵群MKIGaを取得する。その後、その復号化した第一個別中間鍵群MKIGaを個別中間鍵格納部1305aに格納する。

[0095] (3)第二個別中間鍵群取得部1303a

第二個別中間鍵群取得部1303aは、個別情報受信部1301から第二個別情報EMMIIを受信した場合、まず図28に示すような個別鍵格納部1304aから受信装置識別子AIDa及び個別鍵IKaを取得する。そして、受信した第二個別情報EMMIIから、個別鍵格納部1304に格納されていた受信装置識別子AIDaに対応する暗号化第二個別中間鍵群ENCMKIIGaを取得する。その後、個別鍵IKaに基づき、その暗号化第二個別中間鍵群ENCMKIIGaの復号化を行い、第二個別中間鍵群MKIIGaを取得する。その後、その取得した第二個別中間鍵群MKIIGaを個別中間鍵格納部1305aに格納する。

[0096] (4)個別鍵格納部1304a

個別鍵格納部1304aは、図28で示すように、受信装置識別子AIDa及び個別鍵IKa及び暗号化第一個別中間鍵群集合ENCMKIGSaを保持するものである。この個別鍵格納部1304aへは、第一個別中間鍵群取得部1302a及び第二個別中間鍵群取得部1303aからアクセス可能である。また、受信装置識別子AIDaは例えば自然数であり、受信装置識別子AIDbーAIDnのそれぞれと異なる値をとり、個別鍵IKaは、例えば、非特許文献2に記載のDES暗号方式の鍵であり、予め乱数などを用いて生成されたものが埋め込まれており、個別鍵IKbーIKnとは異なる値をとる。

[0097] なお、この個別鍵格納部1304aで格納されている暗号化第一個別中間鍵群集合ENCMKIGSaは、予め鍵発行センタ11により以下のような方法で作成されたものが埋め込まれている。

[0098] 期間識別子PID__1に対応している第一システム秘密変数s__1及びt__1及びu__1及びv__1及びc__1に対して、予め与えられる個別化変数生成式"x＊y＝c__1 mod N"を満たすような2つの個別化変数x、yを生成する。ここで、2つの個別化変数x、yを生成する方法としては、例えば、乱数を用いて一つの個別化変数(例:x)を生成し、その値を個別化変数生成式へ代入することによって、もう一方の個別化変数(例:y)を求める方法などがあり、ランダムな個別化変数xを一つ選ぶと、必ず個別化変数yは存在する。また、個別化変数x、yは、例えば、128ビットの自然数であり、また"＊"は乗算演算のことであり、例えば2＊5は10を意味し、以後同じ意味で用いる。その後、その個別化変数x及びyを用いて、予め与えられる4つの第一個別中間鍵生成式"mkI1＝s__1＊x mod N"、"mkI2＝t__1＊y mod N"、"mkI3＝−u__1＊x mod N"、"mkI4＝−v__1＊y mod N"に基づき4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4を生成する。そして、その4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4から構成される図30で示すような第一個別中間鍵群MKIGaを生成する。そして、この第一個別中間鍵群MKIGaを期間識別子PID__1に対応付けて、鍵発行センタ11が保持する期間鍵PK__1を基に暗号化を行い、暗号化第一個別中間鍵群ENCMKIGaを生成する。他の第一システム秘密変数s__2～s__k及び第二システム秘密変数t__2～t__k及び第三システム秘密変数u__2～u__k及び第四システム秘密変数v__2～v__k及び第五システム秘密変数c__2～c__kに対しても、同様に、個別化変数x及びyを生成し、第一個別中間鍵生成式、を基に、第一個別中間鍵mkI1__2～mkI1__k、mkI2__2～mkI2__k、mkI3__2～mkI3__k、mkI4__2～mkI4__kを生成する。そして、その第一個別中間鍵のそれぞれから構成される第一個別中間鍵群MKIGa__2(＝mkI1__2｜｜mkI2__2｜｜mkI3__2｜｜mkI4__2)、MKIa__3、・・・、MKIa__kを生成する。そして、それぞれの期間識別子PID__2・・・PID__kに対応づけ、期間鍵PK__2・・・PK__nを基に暗号化を行い、暗号化第一個別中間鍵群ENCMKIGa__2、・・・ENCMKIGa__kを生成す

る。最後に、図29で示すような、暗号化第一個別中間鍵群と対応づけた期間識別子の組を連結させた値{(ENCMKIGa__1、PID__1)||(ENCMKIGa__2、PID__2)||、・・・||(ENCMKIGa__k、PID__k)}を暗号化第一個別中間鍵群集合ENCMKIGSaとして予め埋め込まれている。なお、それぞれの暗号化第一個別中間鍵群集合(ENCMKIGSaーENCMKIGSn)は受信装置13aー13n毎に異なる値となるようにする。これは、例えば、それぞれの受信装置13aー13n毎と期間識別子PID__1ーPID__k毎で異なる個別化変数(x、y)を生成し、利用するようにすれば実現出来る。

[0099] (5)個別中間鍵格納部1305a

個別中間鍵格納部1305aは、図31で示すように、第一個別中間鍵群MKIGa及び第二個別中間鍵群MKIIGaを保持するものである。この個別中間鍵格納部1305aへは、第一個別中間鍵群取得部1302a及び第二個別中間鍵群取得部1303aからアクセス可能である。

[0100] (6)共通情報受信部1306

共通情報受信部1306が、サーバ12から共通情報ECMを受信した場合、受信した共通情報ECMを第二選択部1307aに出力する。

[0101] (7)第二選択部1307a

第二選択部1307aは、共通情報受信部1306から共通情報ECMを受信した場合、その共通情報ECMに含まれている共通情報識別子(ECMIDIもしくはECMIDII)を基に、その共通情報ECMが第一共通情報ECMIか第二共通情報ECMIIかを判断する。もし、その共通情報ECMが第一個別情報ECMIの場合、個別中間鍵格納部1305aから第一個別中間鍵群MKIGaを取得し、第一共通情報ECMIと第一個別中間鍵群MKIGaを第一共有鍵取得部1308aへ出力する。反対に、その共通情報ECMが第二個別情報ECMIIの場合、個別中間鍵格納部1305aから第二個別中間鍵群MKIIGaを取得し、第二共通情報ECMIIと第二個別中間鍵群MKIIGaを第二共有鍵取得部1309aへ出力する。

[0102] (8)第一共有鍵取得部1308a

第一共有鍵取得部1308aが、第二選択部1307aから第一個別中間鍵群MKIGa

及び第一共通情報ECMIを受信した場合、まず、第一共通情報ECMIから時変変数PRGを抽出する。その後、その時変変数群PRGから、時変変数r1、r2、r3、r4を抽出し、そして、第一個別中間鍵群MKIGaから第一個別中間鍵mkI1、mkI2、mkI3、mkI4を抽出する。その後、予め与えられる受信装置共通中間鍵生成式"SMK＝(r1＋mkI1)＊(r1＋mkI2)＋(r1＋mkI3)＊(r1＋mkI4) mod N"を基に、共通中間鍵SMKを生成する。そして、第一共通情報ECMIから暗号化共有鍵ENCSKを抽出し、生成した共通中間鍵SMKを基に、その暗号化共有鍵ENCSKを復号化し、共有鍵SKを取得する。そして、その共有鍵SKを出力部1310へ出力する。

[0103] (9)第二共有鍵取得部1309a

第二共有鍵取得部1309aが、第二選択部1307aから第二個別中間鍵群MKIIGa及び第二共通情報ECMIIを受信した場合、まず、第二暗号化共有鍵群ENCSKGから、第二暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENDSK6を抽出する。そして、第二個別中間鍵群MKIIGaに含まれている第二システム秘密鍵に基づいて、その第二システム秘密鍵で共有鍵SKが暗号化された暗号文を、第二暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENDSK6のいずれかから一つを選択し、選択した1つの暗号文を復号化し、共有鍵SKを取得する。その後、その共有鍵SKを出力部1310へ出力する。なお、第二暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENDSK6のいずれかから一つを選択する方法としては、第二共通情報生成部126において、第二暗号化共有鍵群ENCSKGの中に、共有鍵を暗号するのに使用した第二システム秘密鍵を識別する第二システム秘密鍵識別子をそれぞれの第二暗号化共有鍵に対応させるようにして、第二個別中間鍵群MKIIGaにも同様に、含まれている第二システム秘密鍵に対応する第二システム秘密鍵識別子を含ませるようにして、その第二システム秘密鍵識別子を基に、第二暗号化共有鍵ENCSK1ーENDSK6の中から一つを選択する方法などがある。

[0104] (10)出力部1310

出力部1310は、第一共有鍵取得部1308a、もしくは、第二共有鍵取得部1309aのいずれかから共有鍵SKを受信した場合、受信した共有鍵SKを外部へ出力する。

[0105] ＜受信装置13aの動作＞

以上で、受信装置13aの構成について説明を行ったが、ここで受信装置13aの動作について説明する。まず、個別情報群EMMGを受信したときに、第一個別中間鍵群MKIGa及び第二個別中間鍵群MKIIGaを取得する際の動作について図32に示すフローチャートを用いて説明する。次に、共通情報ECMを受信したときに、第一個別中間鍵群MKIGaもしくは第二個別中間鍵群MKIIGaを用いて共有鍵SKを取得する際の動作について図33に示すフローチャートを用いて説明する。

[0106] ≪鍵発行センタ11から個別情報群EMMGを受信した時の動作≫

鍵発行センタ11から個別情報群EMMGを受信した個別情報受信部1301は、受信した個別情報群EMMGの中から、第一個別情報EMMI及び第二個別情報EMMIIを抽出する。(S1301)

個別情報受信部1301は、第一個別情報EMMIを第一個別中間鍵群取得部1302aへ出力し、第二個別情報EMMIIを第二個別中間鍵群取得部1303aへ出力する。(S1302)

第一個別情報EMMIを受信した第一個別中間鍵群取得部1302aは、個別鍵格納部1304aから受信装置識別子AIDa及び個別鍵IKa及び暗号化第一個別中間鍵群集合ENCMKIGSaを取得する。(S1303)

第一個別中間鍵群取得部1302aは、受信した第一個別情報EMMIから、期間識別子PID__i、及び、個別鍵格納部1304に格納されていた受信装置識別子AIDaに対応する暗号化期間鍵ENCPKaを取得する。(S1304)

第一個別中間鍵群取得部1302aは、個別鍵格納部1304に格納されていた個別鍵IKaに基づき、暗号化期間鍵ENCPKaの復号化を行い、期間鍵PK__iを取得する。(S1305)

第一個別中間鍵群取得部1302aは、暗号化第一個別中間鍵群集合ENCMKIGSaの中から、第一個別情報EMMIの中の期間識別子PID__iに対応する暗号化第一個別中間鍵群を取得し、期間鍵PK__iに基づき、その暗号化第一個別中間鍵群の復号化を行い、第一個別中間鍵群MKIGaを取得する。(S1306)

第一個別中間鍵群取得部1302aは、復号化した第一個別中間鍵群MKIGaを個

別中間鍵格納部1305aに格納する。(S1307)

個別情報受信部1301から第二個別情報EMMIIを受信した第二個別中間鍵群取得部1303aは、個別鍵格納部1304aから受信装置識別子AIDa及び個別鍵IKaを取得する。(S1308)

第二個別中間鍵群取得部1303aは、受信した第二個別情報EMMIIから、個別鍵格納部1304に格納されていた受信装置識別子AIDaに対応する暗号化第二個別中間鍵群ENCMKIIGaを取得する。(S1309)

第二個別中間鍵群取得部1303aは、個別鍵IKaに基づき、その暗号化第二個別中間鍵群ENCMKIIGaの復号化を行う。(S1310)

第二個別中間鍵群取得部1303aは、復号化した第二個別中間鍵群MKIIGaを個別中間鍵格納部1305aに格納する。(S1311)

≪サーバ12から共通情報ECMを受信した時の動作≫

サーバ12から共通情報ECMを受信した共通情報受信部1306は、受信した共通情報ECMを第二選択部1307aに出力する。(S1351)

共通情報受信部1306から共通情報ECMを受信した第二選択部1307aは、その共通情報ECMに含まれる共通情報識別子を取得し、もし、その共通情報識別子がECMIDIの場合、その共通情報ECMを第一共通情報ECMIとして、個別中間鍵格納部1305aから第一個別中間鍵群MKIGaを取得し、その第一個別中間鍵群MKIGa及び第一共通情報ECMIを第一共有鍵取得部1308aへ出力し、ステップS1352へ進む。もし、その共通情報識別子がECMIDIIの場合、その共通情報ECMを第二共通情報ECMIIとして、また、個別中間鍵格納部1305aから第二個別中間鍵群MKIIGaを取得し、その第二個別中間鍵群MKIIGa及び第二共通情報ECMIIを第二共有鍵取得部1309aへ出力し、ステップS1356へ進む。(S1352)

第一個別中間鍵群MKIGa及び第一共通情報ECMIを受信した第一共有鍵取得部1308aは、第一共通情報ECMIから時変変数PRGを抽出し、その後、その時変変数群PRGから、時変変数r1、r2、r3、r4を抽出する。そして、第一個別中間鍵群MKIaから第一個別中間鍵mkI1、mkI2、mkI3、mkI4を抽出する。そして、予め与えられる受信装置共通中間鍵生成式"SMK＝(r1＋mkI1)＊(r2＋mkI2)＋(r3＋

mkI3)＊(r4＋mkI4) mod N"を基に、共通中間鍵SMKを計算する。(S1353)

第一共有鍵取得部1308aは、第一共通情報ECMIから暗号化共有鍵ENCSKを抽出し、生成した共通中間鍵SMKを基に、その暗号化共有鍵ENCSKを復号化し、共有鍵SKを取得する。(S1354)

第一共有鍵取得部1308aは、その共有鍵SKを出力部1310へ出力し、ステップS1358へ進む。(S1355)

第二個別中間鍵群MKIIGa及び第二共通情報ECMIIを受信した第二共有鍵取得部1309aは、暗号化共有鍵群ENCSKGから、第二暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENCSK6を抽出する。そして、第二個別中間鍵群MKIIGaに基づいて、その6つの第二暗号化共有鍵ENCSK1、ENCSK2、ENCSK3、ENCSK4、ENCSK5、ENCSK6のいずれか対応する1つの暗号文を復号化し、共有鍵SKを取得する。(S1356)

第二共有鍵取得部1309aは、共有鍵SKを出力部1310へ出力する。(S1357)

出力部1310は、第一共有鍵取得部1308a、もしくは、第二共有鍵取得部1309aの何れかから共有鍵SKを受信した場合、受信した共有鍵SKを外部へ出力する。(S1358)

以上が、鍵配信システム1の構成要素である受信装置13aの構成と動作である。なお、受信装置13aと他の受信装置13bー13nとの相違点は、以下の通りである。

[0107] (i)第一個別中間鍵群取得部1302aで、第一個別中間鍵群を取得するために、個別鍵格納部1304aから得る受信装置識別子及び個別鍵及び暗号化第一個別中間鍵群集合が、それぞれの受信装置13aー13nで異なる。

(ii)第二個別中間鍵群取得部1303aで、第二個別中間鍵群を取得するために、個別鍵格納部1304aから得る受信装置識別子及び個別鍵が、それぞれの受信装置13aー13nで異なる。

[0108] (iii)個別鍵格納部1304aで、格納されている受信装置識別子(AIDaーAIDn)及び個別鍵(IKaーIKn)及び暗号化第一個別中間鍵群集合がそれぞれの受信装置13aー13nで異なる。

[0109] (iv)個別中間鍵格納部1305aで、格納されている第一個別中間鍵群及び第二個

別

中間鍵群がそれぞれの受信装置13a～13nで異なる。

[0110] (v)第二選択部1307aで、個別中間鍵格納部1305aから取得する第一個別中間鍵群及び第二個別中間鍵群がそれぞれの受信装置13a～13nで異なる。

[0111] (vi)第一共有鍵取得部1308aで、共有鍵SKを取得する際に用いる第一個別中間鍵群がそれぞれの受信装置13a～13nで異なる。

[0112] (vii)第二共有鍵取得部1309aで、

第二共有鍵取得部1309aで、共有鍵SKを取得する際に用いる第二個別中間鍵群がそれぞれの受信装置13a～13nで異なる。

[0113] ＜実施形態1の動作検証＞

本実施形態1において、それぞれの受信装置13a～13nには異なる値をとる第一個別中間鍵群MKIGa～MKIGn及び第二個別中間鍵群MKIIGa～MKIIGnが割り当てられているにもかかわらず、全受信装置13a～13nにおいて同じ共有鍵SKが導出出来る理由について説明する。

[0114] まず、第一共通情報ECMI及び第一個別中間鍵群MKIGa～MKIGnを用いる場合について説明する。第一個別中間鍵群MKIGa～MKIGnは、それぞれは予め与えられる4つの第一個別中間鍵生成式を満たす第一個別中間鍵mkI1、mkI2、mkI3、mkI4から構成されている。また、時変変数群PRGは、4つの時変変数生成式を満たすように生成されている。このようにすることで、受信装置共通中間鍵生成式は以下のように変形出来る。

[0115] SMK＝(r1＋mkI1)＊(r2＋mkI2)＋(r3＋mkI3)＊(r4＋mkI4)

＝{s＊(z＋x)＋v＊m}＊{t＊(w＋y)＋u＊n}＋{u＊(z－x)＋t＊m}＊{v＊(w－y)＋s＊n}

＝{s＊(z＋x)＊t＊(w＋y)＋u＊(z－x)＊v＊(w－y)}＋{u＊n＊s＊(z＋x)＋v＊m＊t＊(w＋y)＋s＊n＊u＊(z－x)＋t＊m＊v＊(w－y)}＋u＊v＊m＊n＋s＊t＊m＊n

となる。ここで、“x＊y＝c”という条件を用いることで、

・・＝2＊s＊t＊(z＊w＋c＊n＊m)＋2＊(u＊s＊n＊z＋t＊v＊m＊w)

となり、これは全受信装置13aー13n共通のパラメータのみから成る(つまり、個別化変数x及びyを含まない)。そのため、全受信装置13aー13nにおいて、共通中間鍵SMKが共通の値を導出するようになっている。また、これはサーバ共通中間鍵生成式"SMK＝"2＊s＊t＊(z＊w＋c＊n＊m)＋2＊(u＊s＊n＊z＋t＊v＊m＊w)"と一致する。

[0116] 次に、第二共通情報ECMII及び第二個別中間鍵群MKIIGaーMKIIGnの場合について説明する。第二個別中間鍵群MKIIGaーMKIIGnは、それぞれ予め与えられる複数の第二システム秘密鍵(実施例1の場合6個)のいずれか一つの第二システム秘密鍵から構成されている。また、第二共有情報ECMIIは、共有鍵SKを、複数の第二システム秘密鍵のそれぞれを用いて暗号化した共有鍵SKの暗号文を含んでいる。そのため、複数の第二システム秘密鍵のいずれかの第二システム秘密鍵を保有している全受信装置13aー13nにおいて、共通の共有鍵SKを導出出来るようになっている。

[0117] ＜実施形態1の効果＞

本発明の実施形態1では、すべての受信装置共通の共有鍵SKは、受信装置固有の第一個別中間鍵群及び第二個別中間鍵群から生成されるようにした。そうすることで、万が一、第一個別中間鍵群もしくは第二個別中間鍵群のいずれかの個別情報が偽造されたとしても、もう一方の個別中間鍵を用いて、漏洩元の受信装置が特定出来るようになり、安全性の向上が実現出来る。

[0118] (実施の形態2)

本発明に係る一つの実施の形態としての鍵配信システム2について説明する。実施形態1における鍵配信システム1では、各出力装置13aー13nが共通情報ECMを受信した際に、二つの共有鍵取得方法のいずれかのいずれか一方の方法を選択して共有鍵を取得していたが、実施形態2におけるコンテンツ配信システム2は、ECMを受信した際に、二つの共有鍵取得方法を両方とも利用して共有鍵を取得する点が、実施の形態1と大きく異なる。

[0119] 以下に、本発明のコンテンツ配信システムの一実施形態であるコンテンツ配信システム2の詳細について説明を行う。

[0120] ＜コンテンツ配信システム2の構成＞

鍵配信システム2は、図34に示すように、実施の形態1と同様の通信路10と、実施の形態1とは異なる鍵発行センタ21と、実施の形態1とは異なるサーバ22と、複数の実施の形態1とは異なる受信装置22a－22nから構成される。各々の構成要素の役割については、実施の形態1である鍵配信システム1における鍵発行センタ11とサーバ12と出力装置13a－13nとそれぞれ同じである。

[0121] 以下に、本発明の鍵配信システムの一実施形態である鍵配信システム2の詳細について説明を行う。

[0122] これらの構成要素について詳細に説明する。まず、鍵発行センタ21及びサーバ22及び受信装置23a－23nの構成と動作について図を用いて説明する。

[0123] ＜鍵発行センタ21の構成＞

鍵発行センタ21は、図35に示すように、第四制御部211、第三個別情報生成部212、受信装置対応情報格納部113、システム秘密変数群集合送信部215、個別情報群配信部216、から構成される。なお、受信装置対応情報格納部113に関しては、実施の形態1における鍵配信システム2内の受信装置対応情報格納部113と同様なので、説明を省略する。

[0124] (1)第一制御部211

第一制御部211は、予め与えられる個別情報更新条件を満たした場合、及び、鍵発行センタ23が動作開始した場合に、第三個別情報生成要求REQEMMIIIを第三個別情報生成部212へ出力する。例えば、個別情報更新条件が"ある指定された期間毎(例:1日毎や1年毎)"などの場合、第一制御部211がカウンタなどを備えるなどにより実現可能であり、個別情報更新条件が"外部からある信号を受信した場合"などの場合、第一制御部211が外部信号を受信する受信部を備えるなどにより実現可能である。

[0125] (2)第三個別情報生成部212

第三個別情報生成部212は、図36に示すように、第三システム秘密変数群生成部2121と、第一中間鍵群生成部2122と、から構成される。

[0126] (2－1)第三システム秘密変数群生成部2121

第三システム秘密変数群生成部2121は、第一制御部211から第三個別情報生成要求REQEMMIIIを受信した場合、6個の第一システム秘密変数群識別子SPGIID1ーSPGIID6のそれぞれに対して、第一システム秘密変数群{SPGI1、SPGI2、SPGI3、SPGI4、SPGI5、SPGI6}を生成する。なお、第一システム秘密変数群SPGIi(SPGI1ーSPGI6)のそれぞれの構成については、実施の形態1の鍵配信システム1と同様、図5で示すように、5つの第一システム秘密変数(s__i、t__i、u__i、v__i、c__i:iは1ー6)から構成されている。また、それぞれの第一システム秘密変数SPGI1ーSPGI6は、予め第一システム秘密変数生成式"s__i＊t__i＝u__i＊v__i mod N:iは1ー6"を満たすように生成する。例えば、5つの第一システム秘密変数及びモジュラスNは、例えば128ビットの自然数である。また、ここでのモジュラスNの値は、後述する第三共通情報生成部225、第三共有鍵生成部2308aに予め共通の値として与えられているモジュラスNと同じ値であり、例えば2^{128}などである。ここで、"^"はべき乗演算のことであり、例えば2^{4}は16を意味し、以後同じ意味で用いる。第一システム秘密変数群識別子SPGID1ーSPGIID6は、それぞれの第一システム秘密変数群SPGI1ーSPGI6に対応付けられた識別子であり、例えば、それぞれ異なる自然数である。例えば、6個の第一システム秘密変数群識別子SPGIID1ーSPGIID6は、自然数の1ー6であってもよいし、乱数でも良い。乱数を生成する方法については、非特許文献3が詳しい。そして、図37で示すように、6組の第一システム秘密変数群識別子及び第一システム秘密変数群の組{SPGIID1、SPGI1}{SPGIID2、SPGI2}・・・{SPGIID6、SPGI6}からなる第三システム秘密変数群SPGIIIを生成して、第三システム秘密変数群集合送信部215及び第一中間鍵群生成部2212へ出力する。

[0127] (2ー2)第一中間鍵群生成部2122

第一中間鍵群生成部2122は、第三システム秘密変数群生成部2121から第三システム秘密変数群SPGIIIを受信した場合、受信装置対応情報格納部113にアクセスして、受信装置識別子AIDaーAIDnを取得する。そして、まず受信装置識別子AIDaに対して、第三システム秘密変数群SPGIIIに含まれる6個の第一システム秘密鍵群SPGI1ーSPGI6のうちから、1つの第一システム秘密鍵群を選択する。この1つの

第一システム秘密鍵群の選択方法は、例えば、ランダムに選択する方法などがあり、これは乱数を用いることによって実現出来る。ここでは、例として、受信装置識別子AIDaに対して選択した鍵を、第一秘密変数SPGIiとし(SPGIiはSPGI1ーSPGI6のいずれか)、第一秘密変数SPGIiは、6個の第一システム秘密変数s__i及びt__i及びu__i及びv__i及びc__iから構成されているとする。そして、その6個の第一システム秘密変数s__i、t__i、u__i、v__i、c__iを基に、予め与えられる個別化変数生成式"x＊y＝c__i mod N"を満たすような2つの個別化変数x、yを生成する。ここで、2つの個別化変数x、yを生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。また、個別化変数x、yは、例えば、128ビットの自然数であり、また"＊"は乗算演算のことであり、例えば2＊5は10を意味し、以後同じ意味で用いる。この個別化変数x、yの求め方としては、例えば、個別化変数xをランダムな整数値として生成し、個別化変数生成式"x＊y＝c__i mod N"にその個別化変数xを代入することにより、残りの個別化変数yを求める方法などがあり、ランダムな個別化変数xを一つ選ぶと、必ず個別化変数yは存在する。その後、その個別化変数x及びyを用いて、予め与えられる4つの第一個別中間鍵生成式"mkI1＝s__i＊x mod N"、"mkI2＝t__i＊y mod N"、"mkI3＝−u__i＊x mod N"、"mkI4＝−v__i1＊y mod N"に基づき4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4を生成する。そして、その4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4から構成される図30で示すような第一個別中間鍵群MKIGaを生成する。その後、その個別鍵IKaに基づき、第一個別中間鍵群MKIGaの暗号化を行い、その暗号文を暗号化第一個別中間鍵群ENCMKIGa＝Enc(IKa, MKIGa)とし、受信装置識別子AIDa及び第一秘密変数SPGIiに対する第一システム秘密変数群識別子SPGIIDi(SPGIIDiは1ーSPGIID6のいずれか)に対応付ける。そして、他の受信装置識別子AIDbーAIDnに対しても同様にして、暗号化第一個別中間鍵群ENCMKIGb、・・・、ENCMKIGnとし、それぞれの受信装置識別子AIDbーAIDnと第一システム秘密変数群識別子SPGIIDiに対応付ける。そして、図38で示すような、受信装置識別子AIDaーAIDn及び暗号化第一個別中間鍵群ENCMKIGaーENCMKIGn及び第一システム秘密変数群識別子から構成される第三個別情報EMMIIIを作成し、その第

三個別情報EMMIIIを、個別情報群配信部216に出力する。ここで第一個別中間鍵群を暗号化するのに使用する暗号化アルゴリズムは、例えば、非特許文献2に記載のDES暗号方式などであり、後述する受信装置23a～23nの第三個別中間鍵群取得部1303aで暗号化第一個別中間鍵群を復号化する際に用いる復号化アルゴリズムと同じ方式を用いる。

[0128] (3)システム秘密変数群集合送信部215

システム秘密変数群集合送信部215は、第三個別情報生成部212の第三システム秘密変数群選択部2121から第三システム秘密変数群SPGIIIを受信した場合、その第三システム秘密変数群集合SPGIIIを、サーバ22へ向けて送信する。

[0129] (4)個別情報群配信部216

個別情報群配信部216は、第三個別情報生成部212の第一中間鍵群生成部2122から第三個別情報EMMIIIを受信した場合、その第三個別情報EMMIIIを、受信装置23a～23nへ向けて配信する。

[0130] ＜鍵発行センタ21の動作＞

以上で、鍵発行センタ21の構成について説明を行ったが、ここでは鍵発行センタ21の動作について説明する。ここでは、予め与えられた個別情報更新条件を満たしている場合、もしくは、鍵発行センタ21が動作開始した場合などに、共有鍵を配布、受信するのに必要な鍵情報をサーバ22及び複数の受信装置23a～23nに配信するときの動作について図39に示すフローチャートを用いて説明する。また、第三個別情報生成部212が第三システム秘密変数群SPGIII及び第三個別情報EMMIIIを生成するときの動作の詳細について図40に示すフローチャートを用いて説明する。

[0131] ≪鍵発行センタ21による鍵情報配信時の動作≫

第一制御部211は、第三個別情報生成部212へ第三個別情報生成要求REQEMMIIIを出力する。(S2101)

第三個別情報生成部212は、図40で示すようなフローチャート(下記で詳細を説明)に従って、第三システム秘密変数群SPGIII及び第三個別情報EMMIIIを生成し、第三システム秘密変数群SPGIIIを第三システム秘密変数群集合送信部215へ出力し、第三個別情報EMMIIIを第三個別情報配信部216へ出力する。(S2102)

第三システム秘密変数群SPGIIIを受信した第三システム秘密変数群集合送信部215は、その第三システム秘密変数群SPGIIIをサーバ22へ送信する。(S2103)

第三個別情報EMMIIIを受信した第三個別情報配信部216は、その第三個別情報EMMIIIを受信装置23aー23nへ配信し、終了する。(S2104)

≪第三システム秘密変数群SPGIIIS及び第三個別情報EMMIIIを生成時の動作(ステップS2102の詳細説明)≫

第三個別情報生成要求REQEMMIIIを受信した第三システム秘密変数群生成部2121は、それぞれ5つの第一システム秘密変数(s__i、t__i、u__i、v__i、c__i:iは1ー6)からなる、第一システム秘密変数群{SPGI1、SPGI2、SPGI3、SPGI4、SPGI5、SPGI6}を生成し、第一システム秘密変数群識別子SPGIID1ーSPGIID6のそれぞれに対して対応づける。(S21021)

第三システム秘密変数群生成部2121は、6組の第一システム秘密変数群識別子及び第一システム秘密変数群の組{SPGIID1、SPGI1}{SPGIID2、SPGI2}・・・{SPGIID6、SPGI6}からなる第三システム秘密変数群SPGIIIを生成して、第三システム秘密変数群集合送信部215及び第一中間鍵群生成部2212へ出力する。(S21022)

第三システム秘密変数群SPGIIIを受信した第一中間鍵群生成部2122は、受信装置対応情報格納部113にアクセスして、受信装置識別子AIDaーAIDnを取得する。(S21023)

第三システム秘密変数群SPGIIIを受信した第一中間鍵群生成部2122は、第三システム秘密変数群SPGIIIに含まれる6個の第一システム秘密鍵群SPGI1ーSPGI6のうちから、1つの第一システム秘密鍵群SPGIi(iは1ー6)を選択し、5個の第一システム秘密変数s__i及びt__i及びu__i及びv__i及びc__iを抽出する。(S21024)

第一中間鍵群生成部2122は、5個の第一システム秘密変数s__i、t__i、u__i、v__i、c__iを基に、予め与えられる個別化変数生成式"x＊y＝c__i mod N"を満たすような2つの個別化変数x、yを生成する。(S21025)

第一中間鍵群生成部2122は、その個別化変数x及びyを用いて、予め与えられる4つの第一個別中間鍵生成式"mkI1＝s__i＊x mod N"、"mkI2＝t__i＊y mo

d N"、"mkI3＝−u__i＊x mod N"、"mkI4＝−v__i1＊y mod N"に基づき4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4を生成する。そして、その4個の第一個別中間鍵mkI1、mkI2、mkI3、mkI4から構成される図30で示すような第一個別中間鍵群MKIGaを生成する。(S21026)

第一中間鍵群生成部2122は、個別鍵に基づき、第一個別中間鍵群の暗号化を行い、その暗号文を暗号化第一個別中間鍵群とし、まだ暗号化第一個別中間鍵群が割り当てられていない受信装置識別子に対して、割り当てる。(S21027)

第一中間鍵群生成部2122は、全ての受信装置識別子AIDa～AIDnに対して暗号化第一個別中間鍵群が割り当てられたら、ステップS21029へ進む。もし、全ての受信装置識別子AIDa～AIDnに対して暗号化第一個別中間鍵群が割り当てられたら、ステップ21024に戻る。(S21028)

第一中間鍵群生成部2122は、受信装置識別子AIDa～AIDn及び暗号化第一個別中間鍵群ENCMKIGa～ENCMKIGn及び第一システム秘密変数群識別子から構成される第三個別情報EMMIIIを作成し、その第三個別情報EMMIIIを、個別情報群配信部216に出力する。終了する。(S21029)

以上が、鍵配信システム2の構成要素である鍵発行センタ21の構成と動作である。続いて、サーバ22の構成と動作について説明を行う。

[0132] ＜サーバ22の構成＞

サーバ22は、図41に示すように、システム秘密変数群集合受信部221、システム秘密変数群格納部222、共有鍵生成部123、第三共通情報生成部225、共通情報配信部227、とから構成される。なお、共有鍵生成部123に関しては、実施の形態1の鍵配信システム1における共有鍵生成部123と同じであるため、説明は省略する。

[0133] (1)システム秘密変数群集合受信部221

システム秘密変数群集合受信部221が、鍵発行センタ21から第三システム秘密変数群集合SPGIIISを受信した場合、受信した第三システム秘密変数群集合SPGIIISを、図42で示すようなシステム秘密変数群格納222に格納し、共有鍵生成部123へ共有鍵生成要求REQSKを出力する。

[0134] (2)システム秘密変数群格納部222

システム秘密変数群格納部222は、図42で示すように第三システム秘密変数群集合SPGIIISを格納するものである。

[0135] (3)第三共通情報生成部225

第三共通情報生成部225は、共通情報生成部選択部124から共有鍵SKを受信した場合、まず、システム秘密変数群格納部222にアクセスし、第三システム秘密変数群SPGIIIを取得し、その中から6組の第一システム秘密変数識別子と第一システム秘密変数群を抽出する。そして、一組目の第一システム秘密変数識別子SPGIID1と第一システム秘密変数群SPGI1に対して、6個の第一システム秘密変数s__1、t__1、u__1、v__1、c__1を抽出する。その後、4つの乱数z、w、m、nを生成する。ここで、乱数z、w、m、nを生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。また、乱数z、w、m、nは、例えば、それぞれ128ビットの自然数である。そして、予め与えられる4つの時変変数生成式"r1＝s__1＊z＋v__1＊m mod N"、"r2＝t__1＊w＋u__1＊n N"、"r3＝u__1＊z＋t__1＊m mod N"、"r4＝v__1＊w＋s__1＊n N"を基に、4つの時変変数r1、r2、r3、r4を生成する。そして、生成した時変変数r1、r2、r3、r4から構成される、図20で示すような時変変数群PRGを生成し(これを時変変数PRG1とする)、その時変変数群PRGを第一システム秘密変数識別子SPGIID1に対応付ける。その後、共通中間鍵SMKを、予め与えられるサーバ共通中間鍵生成式"SMK＝2＊s__1＊t__1＊(z＋w＋c__1＋n＊m)＋2＊(u__1＊s__1＊n＊z＋t__1＊v__1＊m＊w) mod N"に基づいて生成する。最後に、その共通中間鍵SMKに基づいて、受け取った共有鍵SKの暗号化を行い、暗号買共有鍵ENCSKを生成し(これを共有中間鍵ENCSK1とする)、その暗号化共有鍵ENCSKを第一システム秘密変数識別子SPGIID1及び時変変数群PRGに対応付ける。そして、他の組の第一システム秘密変数識別子SPGIID2ーSPGIID6と第一システム秘密変数群SPGI2ーSPGI6に対して、SPGIID1と全く同様に、時変変数群PRG2ーPRG6と暗号買共有鍵ENCSK2ーENCSK6を作成する。そして、第一システム秘密変数識別子SPGIID1ーSPGIID6と時変変数群PRG1ーPRG6と暗号買共有鍵ENCSK1ーENCSK6からなる、図43で示すような、第三共通情報ECMIIIを作成し、共通情報配信部へに出力する。ここで共有鍵SK

の暗号化に使用する暗号化アルゴリズムは、例えば、DES暗号方式などであり、後述する受信装置13a－13nの各第三共有鍵取得部2308aにおいて暗号化共有鍵ENCSKを復号化するのに用いる復号化アルゴリズムと同じ方式を用いる。

[0136] (4)共通情報配信部227

共通情報配信227は、第三共通情報生成部225から第三共通情報ECMIIIを受信した場合、受信装置23a－23nへその第三共通情報ECMIIIを配信する。

[0137] ＜サーバ22の動作＞

以上で、サーバ22の構成について説明を行ったが、ここでサーバ22の動作について説明する。まず、鍵発行センタ21から共有鍵SKを配信する際に用いる第三システム秘密変数群集合SPGIIISを受信した際の動作について図44に示すフローチャートを用いて説明する。次に、システム秘密変数群集合受信部221から共有鍵生成要求REQSKを受信した場合、もしくは、予め与えられた共有鍵更新条件を満たした場合、サーバ22が受信装置23a－23nへ新たな共有鍵SKを配信する際の動作について図45に示すフローチャートを用いて説明する。

[0138] ≪鍵発行センタ21から第三システム秘密変数群集合SPGIIISを受信した時の動作≫

システム秘密変数群集合受信部221は、受信した第三システム秘密変数群集合SPGIIISをシステム秘密変数群格納部222へ格納し、終了する。(S2202)

≪サーバ22が受信装置23a－23nへ、新たな共有鍵SKを配信する時の動作≫

共有鍵生成部123は、共有鍵SKを生成し、第三共通情報生成部225へ出力する。(S2251)

第三共通情報生成部225は、システム秘密変数群格納部222にアクセスし、第三システム秘密変数群SPGIIIを取得し、その中から6組の第一システム秘密変数識別子と第一システム秘密変数群を抽出する。(S2252)

第三共通情報生成部225は、まだ時変変数群及び暗号化共有鍵を生成していない一組の第一システム秘密変数識別子と第一システム秘密変数群に対して、6個の第一システム秘密変数s__i、t__i、u__i、v__i、c__iを抽出し、その後、4つの乱数z、w、m、nを生成する。(S2253)

第三共通情報生成部225は、予め与えられる4つの時変変数生成式"r1＝s__i＊z＋v__i＊m mod N"、"r2＝t__i＊w＋u__i＊n N"、"r3＝u__i＊z＋t__i＊m mod N"、"r4＝v__i＊w＋s__i＊n N"を基に、4つの時変変数r1、r2、r3、r4を生成する。(S2254)

第三共通情報生成部225は、生成した時変変数r1、r2、r3、r4から構成される、時変変数群PRGを生成する。(S2255)

第三共通情報生成部225は、共通中間鍵SMKを、予め与えられるサーバ共通中間鍵生成式"SMK＝2＊s__i＊t__i＊(z＋w＋c__i＋n＊m)＋2＊(u__i＊s__i＊n＊z＋t__i＊v__i＊m＊w) mod N"に基づいて生成する。(S2256)

第三共通情報生成部225は、共通中間鍵SMKに基づいて、受け取った共有鍵SKの暗号化を行い、暗号買共有鍵ENCSKを生成し、その暗号化共有鍵ENCSKを第一システム秘密変数識別子SPGIID1及び時変変数群PRGに対応付ける。(S2257)

第三共通情報生成部225は、全ての組の第一システム秘密変数識別子SPGIID1ーSPGIID6に対して、時変変数群PRG1ーPRG6と暗号化共有鍵ENCSK1ーENCSK6を生成したら、ステップS2259へ進む。全ての組の第一システム秘密変数識別子SPGIID1ーSPGIID6に対して、時変変数群PRG1ーPRG6と暗号化共有鍵ENCSK1ーENCSK6を生成していなかったら、ステップS2252へ戻る。(S2258)

第三共通情報生成部225は、第一システム秘密変数識別子SPGIID1ーSPGIID6及び時変変数群PRG1ーPRG6及び暗号化共有鍵ENCSK1ーENCSK6からなる、第三共通情報ECMIIIを作成し、共通情報配信部227へに出力する。(S2259)

共通情報配信227は、受信装置23aー23nへ第三共通情報ECMIIIを配信する。終了する。(S2260)

以上が、鍵配信システム2の構成要素であるサーバ22の構成と動作である。続いて、受信装置23aー23nの構成と動作について説明を行う。まず、受信装置23aの構成と動作について説明を行い、次に、受信装置23aと他の受信装置23bー23nとの相違点について述べる。

[0139] ＜受信装置23aの構成＞

受信装置23aは、図46に示すように、個別情報受信部2301、第三個別中間鍵群取得部2302a、個別鍵格納部2304a、個別中間鍵格納部2305a、共通情報受信部2306a、第三共有鍵取得部2308a、出力部1310、とから構成される。ここで、第三個別中間鍵群取得部2302a、個別鍵格納部2304a、個別中間鍵格納部2305a、共通情報受信部2306a、第三共有鍵取得部2308a、は受信装置23a固有の構成要素であり、個別情報受信部2301、出力部1310、は受信装置23aー23nにおいて共通の構成要素である。

[0140] (1)個別情報受信部2301

個別情報受信部2301が、サーバ22から、第三個別情報群EMMIIIを受信した場合、受信した第三個別情報EMMIIIを第三個別中間鍵群取得部2302aへ出力する。

[0141] (2)第三個別中間鍵群取得部2302a

第三個別中間鍵群取得部2302aは、個別情報受信部2301から第三個別情報EMMIIIを受信した場合、まず図47に示すような個別鍵格納部2304aから受信装置識別子AIDa及び個別鍵IKaを取得する。そして、受信した第三個別情報EMMIIIから、個別鍵格納部2304aに格納されていた受信装置識別子AIDaに対応する暗号化第一中間鍵群ENCMKIGaを取得する。その後、個別鍵IKaを基に、暗号化第一中間鍵群ENCMKIGaの復号化を行い、第一中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDiを取得する。最後に、その第一中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDiを、図48で示すような個別中間鍵格納部2305aへに格納する。

[0142] (3)個別鍵格納部2304a

個別鍵格納部2304aは、図47で示すように、受信装置識別子AIDa及び個別鍵IKaを保持するものである。

[0143] (4)個別中間鍵格納部2305a

個別中間鍵格納部2305aは、図48で示すように、第一個別中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDiを保持するものである。

[0144] (5)共通情報受信部2306a

共通情報受信部2306aが、サーバ22から第三共通情報ECMIIIを受信した場合、個別中間鍵格納部2305aにアクセスし、第一個別中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDiを取得する。そして、第三共通情報ECMIIIの中から、第一システム秘密変数群識別子SPGIIDiと一致する時変変数群PRGi及び暗号化共有鍵ENCSKiを抽出する。その後、第一個別中間鍵群MKIGa及び時変変数群PRGi及び暗号化共有鍵ENCSKiを第三共有鍵取得部2308aへ出力する。

[0145] (6)第三共有鍵取得部2308a

第三共有鍵取得部2308aが、共通情報受信部2306aから第一個別中間鍵群MKIGa及び時変変数群PRGi及び暗号化共有鍵ENCSKiを受信した場合、その時変変数群PRGiから、時変変数r1、r2、r3、r4を抽出する。そして、第一個別中間鍵群MKIGaから第一個別中間鍵mkI1、mkI2、mkI3、mkI4を抽出する。その後、予め与えられる受信装置共通中間鍵生成式"SMK＝(r1＋mkI1)＊(r1＋mkI2)＋(r1＋mkI3)＊(r1＋mkI4) mod N"を基に、共通中間鍵SMKを生成する。そして、生成した共通中間鍵SMKを基に、暗号化共有鍵ENCSKiを復号化し、共有鍵SKを取得する。そして、その共有鍵SKを出力部1310へ出力する。

[0146] ＜受信装置23aの動作＞

以上で、受信装置23aの構成について説明を行ったが、ここで受信装置23aの動作について説明する。まず、第三個別情報群EMMIIIを受信したときに、第一個別中間鍵群MKIGaを取得する際の動作について図49に示すフローチャートを用いて説明する。次に、第三共通情報ECMIIIを受信したときに、第一個別中間鍵群MKIGaを用いて共有鍵SKを取得する際の動作について図50に示すフローチャートを用いて説明する。

[0147] ≪鍵発行センタ21から第三個別情報EMMIIIを受信した時の動作≫

鍵発行センタ21から第三個別情報群EMMIIIを受信した個別情報受信部2301は、第三個別情報EMMIIIを第三個別中間鍵群取得部2302aへ出力する。(S2301)

第三個別情報EMMIIIを受信した第三個別中間鍵群取得部2302aは、個別鍵格納部2304aから受信装置識別子AIDa及び個別鍵IKaを取得する。(S2302)

第三個別中間鍵群取得部2302aは、受信した第三個別情報EMMIIIから、個別鍵格納部2304に格納されていた受信装置識別子AIDaに対応する暗号化第一中間鍵ENCMKIa及び第一システム秘密変数群識別子SPGIIDaを取得する。(S2303)

第三個別中間鍵群取得部2302aは、個別鍵格納部2304に格納されていた個別鍵IKaに基づき、暗号化第一中間鍵ENCMKIaの復号化を行い、第一中間鍵MKIaを取得する。(S2304)

第三個別中間鍵群取得部2302aは、第一個別中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDaを個別中間鍵格納部2305aに格納する。終了する。(S2304)

≪サーバ22から第三共通情報ECMIIIを受信した時の動作≫

サーバ22から第三共通情報ECMIIIを受信した共通情報受信部2306aは、個別中間鍵格納部2305aから第一個別中間鍵群MKIGa及び第一システム秘密変数群識別子SPGIIDaを取得する。(S2351)

共通情報受信部2306aは、第三共通情報ECMIIIの中から、第一システム秘密変数群識別子SPGIIDaに対応する第一システム秘密変数群識別子SPGIIDaと一致する時変変数群PRGi及び暗号化共有鍵ENCSKiを抽出する。(S2352)

共通情報受信部2306aは、第一個別中間鍵群MKIGa及び時変変数群PRGi及び暗号化共有鍵ENCSKiを第三共有鍵取得部2308aへ出力する。(S2353)

第三共有鍵取得部2308aは、時変変数群PRGiから、時変変数r1、r2、r3、r4を抽出する。(S2354)

第三共有鍵取得部2308aは、第一個別中間鍵群MKIGaから第一個別中間鍵mkI1、mkI2、mkI3、mkI4を抽出する。(S2355)

第三共有鍵取得部2308aは、予め与えられる受信装置共通中間鍵生成式"SMK＝(r1＋mkI1)＊(r1＋mkI2)＋(r1＋mkI3)＊(r1＋mkI4) mod N"を基に、共通中間鍵SMKを生成する。(S2356)

第三共有鍵取得部2308aは、生成した共通中間鍵SMKを基に、暗号化共有鍵ENCSKiを復号化し、共有鍵SKを取得する。(S2357)

第三共有鍵取得部2308aは、その共有鍵SKを出力部1310へ出力する。(S2358)

出力部1310は、共有鍵SKを受信した場合、受信した共有鍵SKを外部へ出力する。(S2359)

以上が、鍵配信システム2の構成要素である受信装置23aの構成と動作である。なお、受信装置23aと他の受信装置23bー23nとの相違点は、以下の通りである。

[0148] (i)第三個別中間鍵群取得部2302aで、第三個別中間鍵群を取得するために、個別鍵格納部2304aから得る受信装置識別子及び個別鍵が、それぞれの受信装置23aー23nで異なる。

[0149] (ii)個別鍵格納部2304aで、格納されている受信装置識別子(AIDaーAIDn)及び個別鍵(IKaーIKn)がそれぞれの受信装置23aー23nで異なる。

[0150] (iii)個別中間鍵格納部2305aで、格納されている第一個別中間鍵群及び第一システム秘密変数群識別子がそれぞれの受信装置23aー23nで異なる。

[0151] (iv)共通情報受信部2306aで、個別中間鍵格納部2305aから取得する第一個別中間鍵群及び第一システム秘密変数群識別子がそれぞれの受信装置23aー23nで異なる。

[0152] (v)第三共有鍵取得部2308aで、共有鍵SKを取得する際に用いる第一個別中間鍵群がそれぞれの受信装置13aー13nで異なる。

[0153] <実施形態2の動作検証>

本実施形態2において、それぞれの受信装置23aー23nには異なる値をとる第一個別中間鍵群MKIGaーMKIGnが割り当てられているにもかかわらず、全受信装置23aー23nにおいて同じ共有鍵SKが導出出来る理由については、実施形態1と同様の理由である。

[0154] <実施形態2の効果>

本発明の実施形態2では、すべての受信装置共通の共有鍵SKは、受信装置固有の第三個別中間鍵から生成されるようにした。そうすることで、第三個別中間鍵を埋め込んだ不正な受信装置に対しても、漏洩元の受信装置が特定出来るようになった。

[0155] ＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

[0156] (1)通信路10は、地上波又は衛星等の放送網であっても良い。

(2)実施形態1において、図34で示すように、鍵発行センタ11は可搬媒体15内へシステム秘密変数群集合SPGSを記録して、その可搬媒体15をサーバ12へ配布し、可搬媒体15を受け取ったサーバ12は可搬媒体15内に記録されているシステム秘密変数群集合SPGSを読み取ることによって、システム秘密変数群集合SPGSを取得するようにしても良い。ここで、可搬媒体15は、例えば、フレキシブルディスクやCD−ROMやDVD−RAM等の可搬記録媒体である。これによって、鍵発行センタ11とサーバ12が通信路を介して接続されている必要がなくなる。なお、実施形態2においても、同様に実現可能である。

[0157] (3)実施形態1において、鍵発行センタ11が、もう一つ余分に第一個別中間鍵群を生成し、サーバ12へシステム秘密変数群SPGに加え、その第一個別中間鍵群を配布するようにして、サーバ12のシステム秘密変数群格納部122は、さらに、第一個別中間鍵群を格納するようにして、図35で示すように、サーバ12の時変変数群生成部1251は、共通中間鍵取得部1252へ乱数z、w、m、nの代わりに、時変変数群PRGを出力するようにして、サーバ12の共通中間鍵取得部1252は、時変変数群生成部1251から時変変数群PRGを受け取った場合、まず、システム秘密変数群格納部122にアクセスし、第一個別中間鍵群を取得し、その中から第一個別中間鍵mkI1、mkI2、mkI3、mkI4を取得し、また、受信した時変変数群PRGの中から、時変変数r1、r2、r3、r4を抽出し、その後、共通中間鍵SMKを、予め与えられる受信装置共通中間鍵生成式"SMK＝(r1＋mkI1)＊(r1＋mkI2)＋(r1＋mkI3)＊(r1＋mkI4) mod N"を基に生成するようにしてもよい。これによって、サーバ12の第一個別中間鍵群が漏洩した場合にも、サーバ12から鍵漏洩が起こったということを追跡することが出来るようになる。なお、実施形態2においても、同様に実現可能である。

[0158] (4)システム秘密変数生成式と個別化変数生成式と第一個別中間鍵生成式と時変

変数生成式とサーバ共通中間鍵生成式と受信装置共通中間鍵生成式とは、実施形態1及び実施形態2に記載の式だけに限るものではない。受信装置共通中間鍵生成式に、個別化変数生成式及び第一個別中間鍵生成式及び時変変数生成式と、を代入したときの式が、第一共通中間鍵と一致し、また、第一個別中間鍵生成式とが、個別化変数x、yを含み、さらに、時変変数生成式とサーバ共通中間鍵生成式と受信装置共通中間鍵生成式が、個別化変数x、yを含んでいなければ、それで良い。

[0159] (5)1つのシステム秘密変数生成式を用いてシステム秘密変数群SPGを生成していたが、2種類以上のシステム秘密変数生成式を用いてシステム秘密変数群SPGを生成しても良いし、システム秘密変数生成式を使用せずにシステム秘密変数郡SPGを生成しても良い。例えば、システム秘密変数群SPGは乱数であっても良い。

[0160] (6)1つの個別化変数生成式を用いて個別化変数を生成していたが、2種類以上の個別化変数生成式を用いて個別化変数を生成しても良いし、個別化変数生成式を使用せずに個別化変数を生成しても良い。例えば、個別化変数は乱数であっても良い。

[0161] (7)4つの第一個別中間鍵生成式を用いて中間鍵を生成していたが、5種類以上の第一個別中間鍵生成式を用いて第一個別中間鍵を生成しても良いし、3種類以下の第一個別中間鍵生成式を用いて第一個別中間鍵を生成しても良い。

[0162] (8)4つの時変変数生成式を用いて時変変数群PRGを生成していたが、5種類以上の時変変数生成式を用いて時変変数群PRGを生成しても良いし、3種類以下の時変変数生成式を用いて時変変数群PRGを生成しても良いし、さらには、時変変数生成式を使用せずに時変変数群PRGを生成しても良い。例えば、時変変数群PRGは乱数であってもよい。

[0163] (9)1つのサーバ共通中間鍵生成式を用いて共通中間鍵SMKを計算していたが、2種類以上のサーバ共通中間鍵生成式を用いて共通中間鍵SMKを計算しても良い。

[0164] (10)1つの受信装置共通中間鍵生成式を用いて共通中間鍵SMKを計算していたが、2種類以上の受信装置共通中間鍵生成式を用いて共通中間鍵SMKを生成しても良い。

[0165] (11)受信装置共通中間鍵生成式は、全ての受信装置13a～13n、もしくは、受信装置23a～23nにて共通の受信装置共通中間鍵生成式を用いなくても良い。

[0166] (12)実施形態1において、各第一個別中間鍵群MKIGa～MKIGnは、4つの第一個別中間鍵mkI1、mkI2、mkI3、mkI4から構成されていたが、5つ以上の第一個別中間鍵から構成されていても良いし、3つ以下の第一個別中間鍵から構成されていても良い。

[0167] (13)時変変数群PRGは、4つの時変変数r1、r2、r3、r4から構成されていたが、5つ以上の時変変数から構成されていても良いし、3つ以下の時変変数から構成されていても良い。

[0168] (14)いくつか複数の受信装置に、同じ個別鍵や第一個別中間鍵群や第二個別中間鍵群を割り当てても良い。

[0169] (15)実施形態1では、第二システム秘密鍵生成部1141は、6個の第二システム秘密鍵k1、k2、k3、k4、k5、k6、を生成していたが、7つ以上の第二システム秘密鍵を生成しても良いし、5つ以下の第二システム秘密鍵を生成しても良い。例えば、第二システム秘密鍵生成部1141は10個の第二システム秘密鍵k1、k2、k3、k4、k5、k6、k7、k8、k9、k10を生成してもよい。この際、第二システム秘密変数群SPGIIに含まれる第二システム秘密鍵の数が異なることになる。例えば、第二システム秘密鍵生成部1141で10個の第二システム秘密鍵k1、k2、k3、k4、k5、k6、k7、k8、k9、k10を生成した場合、第二システム秘密変数群SPGIIは10個の第二システム秘密鍵k1、k2、k3、k4、k5、k6、k7、k8、k9、k10を含むことになる。

[0170] (16)実施形態1及び実施形態2において、受信装置は、外部へ共有鍵SKを出力していたが、サーバが外部からコンテンツを入力し、共有鍵SKに基づいてコンテンツを暗号化し、その暗号化コンテンツも受信装置へ配信するようにして、受信装置は、暗号化コンテンツを受信して、共有鍵SKに基づいて復号化を行い、コンテンツを取得し、そのコンテンツを外部に出力するようにしても良い。

[0171] (17)実施形態1のサーバ12では、第一共通情報生成部125もしくは第二共通情報生成部126のいずれかを選択し、第一共通情報ECMIもしくは第二共通情報ECMIIのいずれかしか生成していなかったが、サーバ12が、毎回、第一共通情報生成

部125で第一共通情報ECMIを生成し、第二共通情報生成部126で第二共通情報ECMIIを生成し、生成後に、第一共通情報ECMIもしくは第二共通情報ECMIIのいずれかを選択して、受信装置13a－13nへ配信するようにしても良い。

[0172] (18)実施形態1において、鍵発行センタ11が個別情報群EMMGを配信する際には、受信装置13a－13nへ同時に配信しても良いし、各受信装置13a－13n個別に配信しても良い。なお、サーバ12が共通情報ECMを配信する際にも同様に、受信装置13a－13nへ同時に配信しても良いし、各受信装置13a－13n個別に配信しても良い。

[0173] (19)実施形態2において、第三システム秘密鍵群集合SPGIIISは、第一システム秘密鍵群を6個含んでいたが、7個以上含んでいてもよいし、5個以下含んでいても良い。

[0174] (20)実施形態2において、鍵発行センタ21が第三個別情報群EMMIIIを配信する際には、受信装置23a－23nへ同時に配信しても良いし、各受信装置23a－23n個別に配信しても良い。なお、サーバ22が第三共通情報ECMIIIを配信する際にも同様に、受信装置23a－23nへ同時に配信しても良いし、各受信装置23a－23n個別に配信しても良い。

[0175] (21)実施形態1では、サーバ12が受信装置13a－13nへ共通情報ECMを送信していたが、サーバ12と受信装置13a－13nが予め共通の共通情報ECMと共通情報識別子の組を複数保持しており、サーバ12がいずれかの共通情報識別子を受信装置13a－13nへ配信して、受信装置13a－13nでは受信した共通情報識別子を基に、対応する共通情報ECMを取得するようにしても良い。

[0176] (22)実施形態1において、鍵発行センタ11は、受信装置識別子とその受信装置識別子に対応する受信装置に割り当てた第一個別中間鍵群及び第二個別中間鍵群の対応情報を保持するようにして、ある第一個別中間鍵群、もしくは、ある第二個別中間鍵群を基に、割り当てられている受信装置を特定出来るようにしても良い。そのようにすることで、ある不正受信装置が発見された時にも、その不正受信装置に埋め込まれている第一個別中間鍵群、もしくは、ある第二個別中間鍵群を基に、漏洩した受信装置を特定出来るようになる。なお、対応情報は、鍵発行センタ11以外が保

持していても良いし、対応情報は、第一個別中間鍵群、もしくは、第二個別中間鍵群のいずれかと受信装置識別子の組のみを含んでいても良い。また、実施形態2においても、鍵発行センタ21、もしくは、鍵発行センタ21以外が、受信装置識別子とその受信装置識別子に対応する受信装置に割り当てた第一個別中間鍵群と第一システム秘密変数群識別子の対応情報を保持するようにしても、同様のことが実現出来る。さらに、対応情報は、第一個別中間鍵群、もしくは、第一システム秘密変数群識別子のいずれかと受信装置識別子の組のみを含んでいても良い。

[0177] (23)実施形態1において、鍵発行センタ11には第一個別情報生成部及び第二個別情報生成部があったが、第三個別情報生成部や第四個別情報生成部、それ以上の個別情報生成部があってもよく、受信装置13a－13nには第一個別中間鍵群取得部及び第二個別中間鍵群取得部があったが、第三個別中間鍵群取得部や第四個別中間鍵群取得部、それ以上の個別中間鍵群取得部があってもよい。鍵発行センタ11と受信装置13a－13nにおいて、個別情報生成部と個別中間鍵群取得部が同じ数だけ存在し、その同じ種類だけ個別情報識別子があれさえすればよい。

[0178] (24)実施形態1において、サーバ12には第一共通情報生成部及び第二共通情報生成部があったが、第三共通情報生成部や第四共通情報生成部、それ以上の共通情報生成部があってもよく、受信装置13a－13nには第一共有鍵取得部及び第二共有鍵取得部があったが、第三共有鍵取得部や第四共有鍵取得部、それ以上の共有鍵取得部があってもよい。サーバ12と受信装置13a－13nにおいて、共通情報生成部と共有鍵取得部が同じ数だけ存在し、その同じ種類だけ共通情報識別子があれさえすればよい。

[0179] (25)実施形態1において、期間鍵PK_1－PK_kは全受信装置13a－13nにおいて共通の鍵であったが、受信装置毎に個別の鍵であっても良い。

[0180] (26)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、CD、MO、DVD、SDメモリカード、半導体メ

モリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0181] (27)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0182] 本発明にかかる鍵配信システムは、攻撃者によって、ある受信装置の個別鍵を不正に取得され、その個別鍵を用いて不正な受信装置が作成されたとしても、その不正な受信装置のクローン元を追跡出来るという効果を有し、インターネット等の通信路、地上波放送や衛星放送などの放送網を用いて、コンテンツを安全に配信したい場合に有用である。

請求の範囲

[1] 共有鍵を配信する鍵配信システムであって、

前記鍵配信システムは、

前記共有鍵を基に共通情報を生成し、前記共通情報を配信するサーバと、

前記共通情報及び個別中間鍵群集合を基に、前記共有鍵を取得する複数の受信装置と、から構成され、

前記受信装置は、一以上のシステム秘密変数群に基づく一以上の個別中間鍵からなる個別中間鍵群を複数含む前記個別中間鍵群集合を少なくとも異なる二種類以上含む複数の前記個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、

前記サーバと前記受信装置のそれぞれは通信路を介して通信可能であって、

前記サーバは、

前記共有鍵を格納する共有鍵格納部と、

予め与えられた一以上の前記システム秘密変数群からなるシステム秘密変数群集合を格納するシステム秘密変数群格納部と、

前記共有鍵を基に、前記共通情報を生成する複数の共通情報生成部と、

複数の前記共通情報生成部の中から一つを選択する共通情報生成部選択部と、

前記共通情報を複数の前記受信装置に同時に、または、個別に配信する共通情報配信部と、を備え、

前記複数の共通情報生成部は、各々、共通情報生成方法が異なり、前記共通情報生成方法を使用して、前記システム秘密変数群集合及び前記共有鍵に基づき、鍵更新データを作成し、前記共通情報生成方法に対応付けられた共通情報識別子及び前記鍵更新データを含む前記共通情報を生成し、

前記受信装置は、

前記共通情報を受信する共通情報受信部と、

複数の共通情報生成方法の各々に対応する前記個別中間鍵群からなる前記個別中間鍵群集合を格納する個別中間鍵群格納部と、

複数の前記共通情報生成部に対応する複数の共有鍵取得部と、

複数の前記共有鍵取得部の中から一つを選択する共有鍵取得部選択部と、を備え、

前記共有鍵取得部選択部は、前記共通情報受信部で受信した前記共通情報に含まれる前記共通情報識別子に基づき、

前記複数の共有鍵取得部の中から一つを選択し、

前記共有鍵取得部は、前記共通情報識別子に対応した共有鍵取得方法と前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得すること

を特徴とする鍵配信システム。

[2] 複数の前記共通情報生成方法は、第一共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、

前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、

前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記サーバには、一以上の時変変数生成式及び一以上のサーバ共通中間鍵生成式が予め与えられており、

前記受信装置のそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、

前記第一共通情報生成方法は、

一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一システム秘密変数群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、

前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成し、

前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含む、方法であり、

前記第一共有鍵取得方法は、

前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする、請求項1に記載の鍵配信システム。

[3] 前記サーバには、前記複数の個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、

前記サーバは、予め与えられた前記個別中間鍵群集合を格納する個別中間鍵群集合格納部と、を備え、

複数の前記共通情報生成方法は、第一共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、

前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、

前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記サーバには、一以上の時変変数生成式及び一以上の受信装置共通中間鍵生成式が予め与えられており、

前記受信装置のそれぞれには、前記受信装置共通中間鍵生成式が予め与えられており、

前記第一共通情報生成方法は、

一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一個別中間鍵群及び前記時変変数群及び前記受信装置共通中間鍵生成式を基に、共通中間鍵を生成し、

前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成し、

前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含む、方法であ

り、

前記第一共有鍵取得方法は、

前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする、請求項1に記載の鍵配信システム。

[4] 複数の前記共通情報生成方法は、第二共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第二共通情報生成方法と対となる第二共有鍵取得方法を含み、

前記システム秘密変数群集合は、複数の第二システム秘密鍵から成る第二システム秘密鍵群を含み、

前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、

前記第二共通情報生成方法は、

前記第二システム秘密鍵群に含まれる一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生成し、

前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成し、

前記鍵更新データは、前記暗号化共有鍵群を含む、方法であり、

前記第二共有鍵取得方法は、

前記鍵更新データに含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、

前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする、請求項1記載の鍵配信システム。

[5] 前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含み、

前記第二共通情報生成方法は、

前記第二システム秘密鍵群に含まれる複数の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生成し、前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成する方法であることを特徴とする、請求項4に記載の鍵配信システム。

[6] 前記鍵配信システムは、さらに、前記通信路を介して前記受信装置のそれぞれに接続され、個別情報群を配信する鍵発行センタと、を備え、

前記鍵発行センタは、

予め前記受信装置に与えられた一以上の個別鍵を格納する出力装置対応情報格納部と、

前記個別情報を生成する複数の個別情報生成部と、

前記個別情報及び前記個別情報生成部に対応付けられた個別情報識別子の組を二種類以上含む前記個別情報群を、複数の前記受信装置に同時に、または、個別に配信する個別情報群配信部と、を備え、

前記個別情報生成部は、各々、個別情報生成方法が異なり、前記個別情報生成方法を基に、前記個別情報識別子及び前記システム秘密変数群及び前記個別情報を出力し、

前記受信装置は、

予め与えられた前記個別鍵を格納する個別鍵格納部と、

前記個別情報群を受信する個別情報群受信部と、

複数の前記個別情報生成部に対応する複数の個別中間鍵群取得部と、を備え、

前記個別情報受信部は、受信した前記個別情報群に含まれる前記個別情報識別子に基づき、複数の前記個別中間鍵群取得部のそれぞれへ、前記個別情報識別子に対応する前記個別情報を出力し、

前記個別中間鍵取得部は、前記個別情報識別子に対応した個別中間鍵取得方法を使用して、前記個別情報及び前記個別鍵に基づき、前記個別中間鍵群を取得することを特徴とする、請求項1記載の鍵配信システム。

[7] 前記複数の個別情報生成部は、さらに、前記システム秘密変数群を生成し、

前記鍵発行センタは、

前記システム秘密変数群及び前記個別情報生成部に対応付けられた前記個別情報識別子の組を二種類以上含む前記システム秘密変数群集合を前記サーバへ配布するシステム秘密変数群集合送信部と、を備え、

前記サーバは、

配布された前記システム秘密変数群集合を前記システム秘密変数群格納部へ格納するシステム秘密変数群集合受信部と、を備えることを特徴とする、請求項6に記載の鍵配信システム。

[8] 前記鍵発行センタは、前記通信路を介して前記サーバに接続され、

前記システム秘密変数群集合送信部は、前記通信路を介して前記サーバへ前記システム秘密変数群集合を配信し、前記システム秘密変数群集合受信部は、前記通信路を介して前記鍵発行センタから前記システム秘密変数群集合を受信することを特徴とする、請求項6記載の鍵配信システム。

[9] 前記システム秘密変数群集合送信部は、可搬媒体へ前記システム秘密変数群集合を記録し、前記システム秘密変数群集合受信部は、前記可搬媒体に記録された前記システム秘密変数群集合を読み取ることを特徴とする、請求項6記載の鍵配信システム。

[10] 前記鍵発行センタと前記サーバは、予めサーバ鍵を共有しているとし、前記システム秘密変数群集合送信部は、前記サーバ鍵を基に前記システム秘密変数群集合を暗号化して、暗号化データを作成して、前記サーバへ配布し、前記システム秘密変数群集合受信部は、配布された前記暗号化データを前記サーバ鍵を基に復号化し、前記システム秘密変数群集合を取得することを特徴とする、請求項7記載の鍵配信システム。

[11] 複数の前記個別情報生成方法は、第一個別情報生成方法を含み、

複数の前記個別中間鍵取得方法は、前記第一個別情報生成方法と対となる第一個別中間鍵群取得方法を含み、

前記鍵発行センタは、予め与えられる期間鍵及び前記期間鍵に対応付けられた前記第一システム秘密変数群及び前記期間鍵に対応付けられた期間識別子の組を一種類以上格納する期間情報格納部と、を備え、

前記受信装置の前記個別鍵格納部のそれぞれは、前記期間鍵を基に、前記第一個別中間鍵群が暗号化されることにより生成された暗号化第一個別中間鍵群及び前記期間鍵に対応付けられた前記期間識別子の組を一種類以上格納しており、

前記第一個別情報生成方法は、

前記期間情報格納部の中から、一組の前記期間鍵及び前記第一システム秘密変数群及び前記期間識別子を選択し、

各々の前記個別鍵を基に、前記期間鍵を暗号化し、複数の暗号化期間鍵を生成し、

前記個別情報群は、前記複数の暗号化期間鍵を結合した暗号化期間鍵群及び前記期間識別子からなる第一個別情報を含み、

前記第一個別中間鍵群取得方法は、

前記個別鍵に基づき、前記第一個別情報に含まれる前記複数の暗号化期間鍵のいずれか一つの前記暗号化期間鍵を復号化し、前記期間鍵を取得し、

前記個別鍵格納部に含まれる一以上の前記暗号化第一個別中間鍵群の中から、前記期間識別子に対応付けられた前記暗号化第一個別中間鍵群を一つ選択し、

前記期間鍵に基づき、前記暗号化第一個別中間鍵群を復号化することによって、前記第一個別中間鍵群を取得する方法であることを特徴とする、請求項6記載の鍵配信システム。

[12] 複数の前記個別情報生成方法は、第二個別情報生成方法を含み、

複数の前記個別中間鍵取得方法は、前記第二個別情報生成方法と対となる第二個別中間鍵群取得方法を含み、

前記第二個別情報生成方法は、

各々の前記個別鍵に対して、複数の前記第二システム秘密鍵のいずれか一つを選定し、各々の前記個別鍵に基づき、選定した前記第二システム秘密鍵を暗号化し、複数の暗号化第二システム秘密鍵を生成し、

前記個別情報群は、前記複数の暗号化第二システム秘密鍵を結合した暗号化第二システム秘密鍵群を含む第二個別情報を含み、

前記第二個別中間鍵群取得方法は、

前記第二個別情報に含まれる前記複数の暗号化第二システム秘密鍵の中から、前記個別鍵に対応する前記暗号化第二システム秘密鍵を一つ選定し、前記個別鍵に基づき、選定した前記暗号化第二システム秘密鍵を復号化することによって、前記第二システム秘密鍵を取得し、その前記第二システム秘密鍵を前記第二個別中間鍵群とする方法であることを特徴とする、請求項6記載の鍵配信システム。

[13] 前記個別中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする、請求項2記載の鍵配信システム。

[14] 前記時変変数生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする、請求項2記載の鍵配信システム。

[15] 前記サーバ共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする、請求項2記載の鍵配信システム。

[16] 前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする、請求項2記載の鍵配信システム。

[17] 前記第二システム秘密鍵群は、10個の第二システム秘密鍵から成ることを特徴とする、請求項4記載の鍵配信システム。

[18] 共有鍵を配信するサーバと、前記共有鍵を受信する複数の受信装置と、を備える鍵配信システムにおける受信装置であって、

前記受信装置は、

外部から共通情報を受信する共通情報受信部と、

複数の共有鍵取得方法の各々に対応する個別中間鍵群から成る個別中間鍵群集合を格納する個別中間鍵群格納部と、

複数の前記共有鍵取得方法に対応する複数の共有鍵取得部と、

複数の前記共有鍵取得部の中から一つを選択する共有鍵取得部選択部と、を備え、

前記共有鍵取得部選択部は、前記共通情報受信部で受信した前記共通情報に含まれる共通情報識別子に基づき、前記共有鍵取得部を一つ選択し、

前記共有鍵取得部は、前記共通情報識別子に対応した前記共有鍵取得方法及び前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得すること

を特徴とする受信装置。

[19] 複数の前記共有鍵取得方法は、第一共有鍵取得方法を含み、

前記個別中間鍵群集合は、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記受信装置のそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、

前記共通情報は、時変変数群及び暗号化共有鍵からなる第一共通情報を含み、

前記第一共有鍵取得方法は、

前記第一共通情報に含まれる前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする、請求項18記載の受信装置。

[20] 複数の前記共有鍵取得方法は、第二共有鍵取得方法を含み、

前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、

前記共通情報は、前記複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵を暗号化することで生成された一以上の暗号化共有鍵を含む暗号化共有鍵群からなる第二共通情報を含み、

前記第二共有鍵取得方法は、

前記共通第二共通情報に含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、

前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする、請求項18記載の受信装置。

[21] 前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする、請求項20記載の受信装置。

[22] 前記鍵配信システムは、さらに、前記通信路を介して前記受信装置のそれぞれとサーバに接続され、個別情報群を配信する鍵発行センタと、を備え、

前記受信装置は、

予め与えられた個別鍵を格納する個別鍵格納部と、

外部から前記個別情報群を受信する個別情報群受信部と、

複数の個別中間鍵取得方法に対応する複数の個別中間鍵群取得部と、を備え、

前記個別情報受信部は、受信した前記個別情報群に含まれる個別情報識別子に基づき、複数の前記個別中間鍵群取得部のそれぞれへ、前記個別情報群に含まれ前記個別情報識別子に対応する前記個別情報を出力し、

前記個別中間鍵取得部は、前記個別情報識別子に対応した前記個別中間鍵取得方法を使用して、前記個別情報及び前記個別鍵に基づき、前記個別中間鍵群を取得することを特徴とする、請求項18記載の受信装置。

[23] 複数の前記個別中間鍵取得方法は、第一個別中間鍵群取得方法を含み、

前記受信装置の前記個別鍵格納部のそれぞれは、期間鍵を基に、第一個別中間鍵群を暗号化することにより生成される暗号化第一個別中間鍵群及び前記期間鍵に対応付けられた期間識別子の組を一種類以上格納しており、

前記個別情報群は、それぞれの前記個別鍵を基に前記期間鍵を暗号化して生成された複数の暗号化期間鍵を含む暗号化期間鍵群及び前記期間識別子からなる第一個別情報を含み、

前記第一個別中間鍵群取得方法は、

前記個別鍵に基づき、前記第一個別情報に含まれる前記複数の暗号化期間鍵のいずれか一つの前記暗号化期間鍵を復号化し、前記期間鍵を取得し、

前記個別鍵格納部に含まれる一以上の前記暗号化第一個別中間鍵群の中から、前記期間識別子に対応付けられた前記暗号化第一個別中間鍵群を一つ選択し、

前記期間鍵に基づき、前記暗号化第一個別中間鍵群を復号化することによって、前記第一個別中間鍵群を取得する方法であることを特徴とする、請求項19記載の受信装置。

[24] 複数の前記個別中間鍵取得方法は、第二個別中間鍵群取得方法を含み、

前記個別情報群は、それぞれの前記個別鍵を基に、前記第二システム秘密鍵のいずれかを暗号化することによって生成された複数の暗号化第二システム秘密鍵からなる暗号化第二システム秘密鍵群を含む第二個別情報を含み、

前記第二個別中間鍵群取得方法は、

前記第二個別情報に含まれる前記複数の暗号化第二システム秘密鍵の中から、前記個別鍵に対応する前記暗号化第二システム秘密鍵を一つ選定し、前記個別鍵に基づき、選定した前記暗号化第二システム秘密鍵を復号化することによって、前記第二システム秘密鍵を取得し、その前記第二システム秘密鍵を前記第二個別中間鍵群とする方法であることを特徴とする、請求項20記載の受信装置。

[25] 前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする、請求項19記載の受信装置。

[26] 共有鍵を配信するサーバと、通信路を介して接続され、前記共有鍵を受信する処理をコンピュータに実行させるプログラムであって、

外部から共通情報を受信するステップと、

複数の共有鍵取得方法の各々に対応する個別中間鍵群から成る個別中間鍵群集合を格納するステップと、

複数の前記共有鍵取得方法に対応する複数の共有鍵取得ステップと、

前記共通情報受信部で受信した前記共通情報に含まれる共通情報識別子に基づき、前記共有鍵取得部を一つ選択するステップと、をコンピュータに実行させ、

前記共有鍵取得ステップは、前記共通情報識別子に対応した前記共有鍵取得方法及び前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とするプログラム。

[27] 複数の前記共有鍵取得方法は、第一共有鍵取得方法を含み、

前記個別中間鍵群集合は、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記プログラムのそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、

前記共通情報は、時変変数群及び共通中間鍵を基に前記共有鍵を暗号化するこ

とにより生成される暗号化共有鍵からなる第一共通情報を含み、

前記第一共有鍵取得方法は、

前記第一共通情報に含まれる時変変数群、及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする請求項26記載のプログラム。

[28] 複数の前記共有鍵取得方法は、第二共有鍵取得方法を含み、

前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、

前記共通情報は、前記複数の第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵を基に前記共有鍵を暗号化することにより生成される複数の暗号化共有鍵からなる暗号化共有鍵群を含む第二共通情報を含み、

前記第二共有鍵取得方法は、

前記共通第二共通情報に含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、

前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする請求項26記載のプログラム。

[29] 前記個別中間鍵群集合は、複数の第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする請求項28記載のプログラム。

[30] 前記受信装置共通中間鍵生成式には、少なくとも、加算演算及び乗算演算が含まれていることを特徴とする請求項27記載のプログラム。

[31] 請求項26記載のプログラムを記録した媒体。

[32] 共有鍵を配信する鍵配信方法であって、

前記鍵配信方法は、

前記共有鍵を基に共通情報を生成し、前記共通情報を配信する鍵配信ステップと

、

前記共通情報及び個別中間鍵群集合を基に、前記共有鍵を取得する複数の鍵受信ステップと、から構成され、

前記鍵受信ステップには、一以上のシステム秘密変数群に基づく一以上の個別中間鍵からなる個別中間鍵群を複数含む前記個別中間鍵群集合を少なくとも異なる二種類以上含む複数の前記個別中間鍵群集合の中から、いずれか一つの前記個別中間鍵群集合が予め与えられており、

前記鍵配信ステップは、

前記共有鍵を格納するステップと、

予め与えられた一以上のシステム秘密変数群からなるシステム秘密変数群集合を格納するステップと、

前記共有鍵を基に、前記共通情報を生成する複数の共通情報生成ステップと、

複数の前記共通情報生成ステップの中から一つを選択するステップと、

前記共通情報を複数の前記受信装置に同時に、または、個別に配信するステップと、を含み、

前記複数の共通情報生成ステップは、各々、共通情報生成方法が異なり、前記共通情報生成方法を使用して、前記システム秘密変数群集合及び前記共有鍵に基づき、鍵更新データを作成し、前記共通情報生成方法に対応付けられた共通情報識別子及び前記鍵更新データを含む前記共通情報を生成し、

前記鍵受信ステップは、

前記共通情報を受信するステップと、

複数の共通情報生成方法の各々に対応する前記個別中間鍵群からなる前記個別中間鍵群集合を格納するステップと、

複数の前記共通情報生成部に対応する複数の共有鍵取得ステップと、

前記共通情報受信部で受信した前記共通情報に含まれる前記共通情報識別子に基づき、複数の前記共有鍵取得ステップの中から一つを選択するステップと、を含み

、

前記共有鍵取得ステップは、前記共通情報識別子に対応した共有鍵取得方法と

前記個別中間鍵群に基づき、前記共通情報を使用して、前記共有鍵を取得することを特徴とする鍵配信方法。

[33] 複数の前記共通情報生成方法は、第一共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、

前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、

前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記鍵配信ステップには、一以上の時変変数生成式及び一以上のサーバ共通中間鍵生成式が予め与えられており、

前記鍵受信ステップのそれぞれには、一以上の受信装置共通中間鍵生成式が予め与えられており、

前記第一共通情報生成方法は、

一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一システム秘密変数群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、

前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成する方法であり、

前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含み、

前記第一共有鍵取得方法は、

前記時変変数群及び前記第一個別中間鍵群及び前記受信装置共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする、請求項32記載の鍵配信方法。

[34] 前記鍵配信ステップは、前記複数の前記個別中間鍵群集合の中から、いずれか一

つの前記個別中間鍵群集合が予め与えられており、

前記鍵受信ステップは、予め与えられた前記個別中間鍵群集合を格納するステップと、を含み、

複数の前記共通情報生成方法は、第一共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第一共通情報生成方法と対となる第一共有鍵取得方法を含み、

前記システム秘密変数群集合は、一以上の第一システム秘密変数から成る第一システム秘密変数群を含み、

前記個別中間鍵群集合は、前記第一システム秘密変数群及び一以上の第一個別中間鍵生成式に基づき生成される、一以上の第一個別中間鍵から成る第一個別中間鍵群を含み、

前記サーバには、一以上の時変変数生成式及び一以上の共通中間鍵生成式が予め与えられており、

前記鍵受信ステップのそれぞれには、前記共通中間鍵生成式が予め与えられており、

前記第一共通情報生成方法は、

一以上の乱数からなる乱数群を生成し、前記乱数群及び前記第一システム秘密変数群及び前記時変変数生成式を基に、一以上の時変変数から成る時変変数群を生成し、前記第一個別中間鍵群及び前記乱数群及び前記サーバ共通中間鍵生成式を基に、共通中間鍵を生成し、

前記共通中間鍵を基に、前記共有鍵を暗号化して、暗号化共有鍵を生成する方法であり、

前記鍵更新データは、前記時変変数群及び前記暗号化共有鍵を含み、

前記第一共有鍵取得方法は、

前記時変変数群及び前記第一個別中間鍵群及び前記共通中間鍵生成式を基に、前記共通中間鍵を生成し、

前記共通中間鍵を基に、前記暗号化共有鍵の復号化を行い、前記共有鍵を取得する方法であることを特徴とする、請求項33記載の鍵配信方法。

[35] 複数の前記共通情報生成方法は、第二共通情報生成方法を含み、

複数の前記共有鍵取得方法は、前記第二共通情報生成方法と対となる第二共有鍵取得方法を含み、

前記システム秘密変数群集合は、複数の第二システム秘密鍵から成る第二システム秘密鍵群を含み、

前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一以上の前記第二システム秘密鍵から成る第二個別中間鍵群を含み、

前記第二共通情報生成方法は、

前記第二システム秘密鍵群に含まれる一以上の前記第二システム秘密鍵のそれぞれを基に、前記共有鍵の暗号化を行い、複数の暗号化共有鍵を生成し、

前記複数の暗号化共有鍵を結合した暗号化共有鍵群を生成する方法であり、

前記鍵更新データは、前記暗号化共有鍵群を含み、

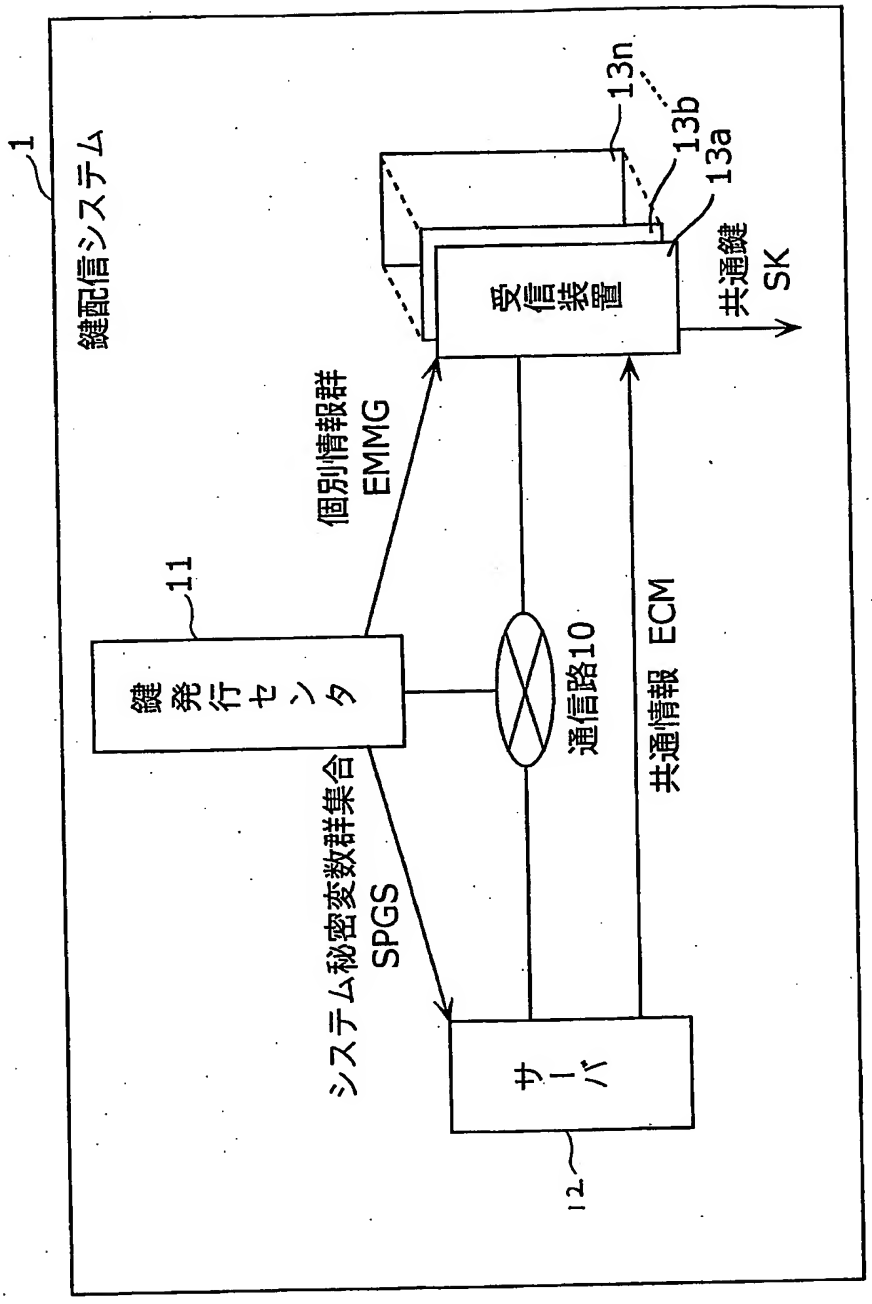
前記第二共有鍵取得方法は、

前記鍵更新データに含まれる前記暗号化共有鍵群の中から、前記第二個別中間鍵群に含まれる前記第二システム秘密鍵のいずれかに対応する一つの前記暗号化共有鍵を選定し、

前記第二システム秘密鍵を基に、選定した前記暗号化共有鍵を復号化することにより、前記共有鍵を取得する方法であることを特徴とする、請求項32記載の鍵配信方法。

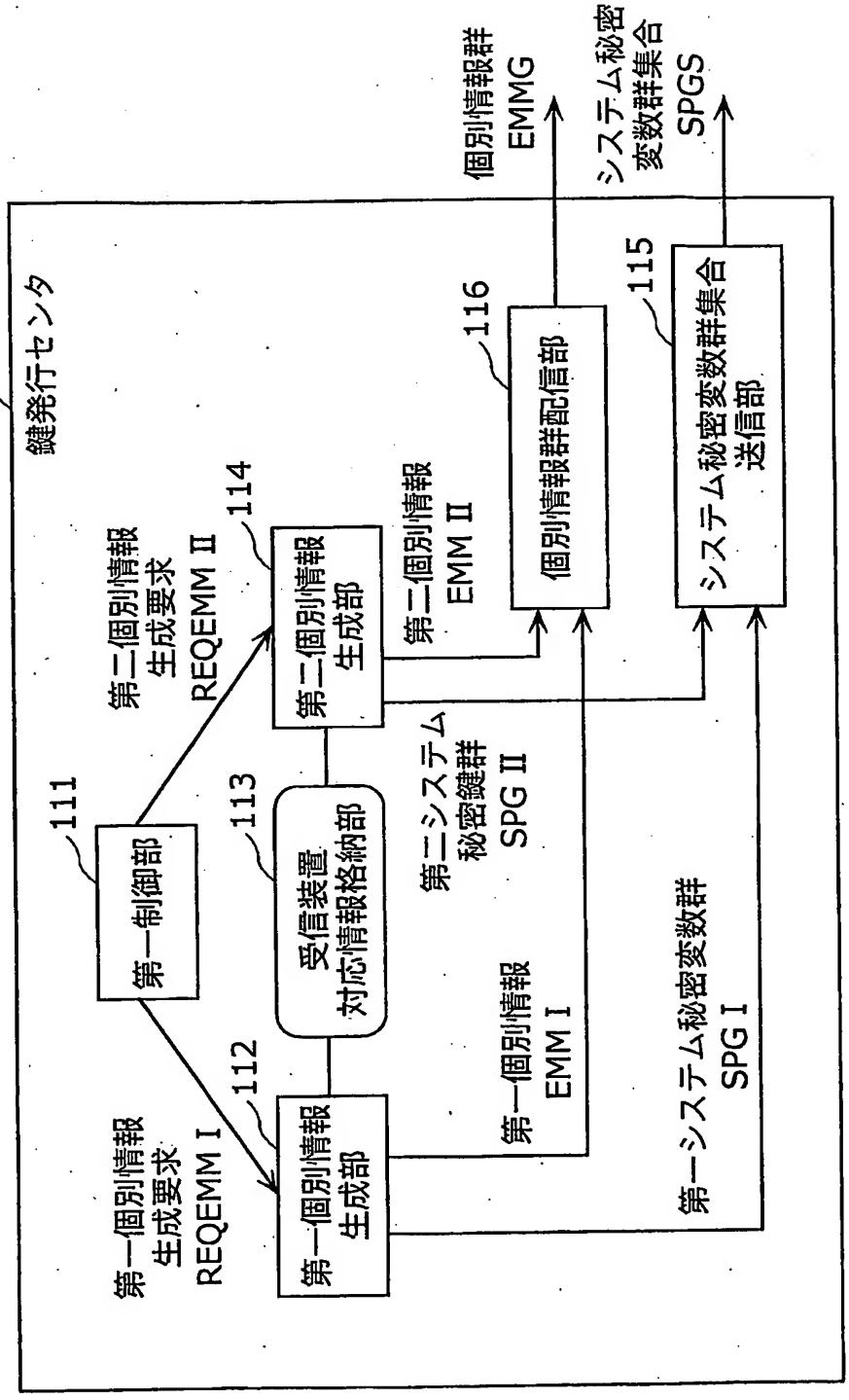
[36] 前記個別中間鍵群集合は、複数の前記第二システム秘密鍵のいずれか一つの前記第二システム秘密鍵から成る第二個別中間鍵群を含むことを特徴とする、請求項35記載の鍵配信方法。

【図1】

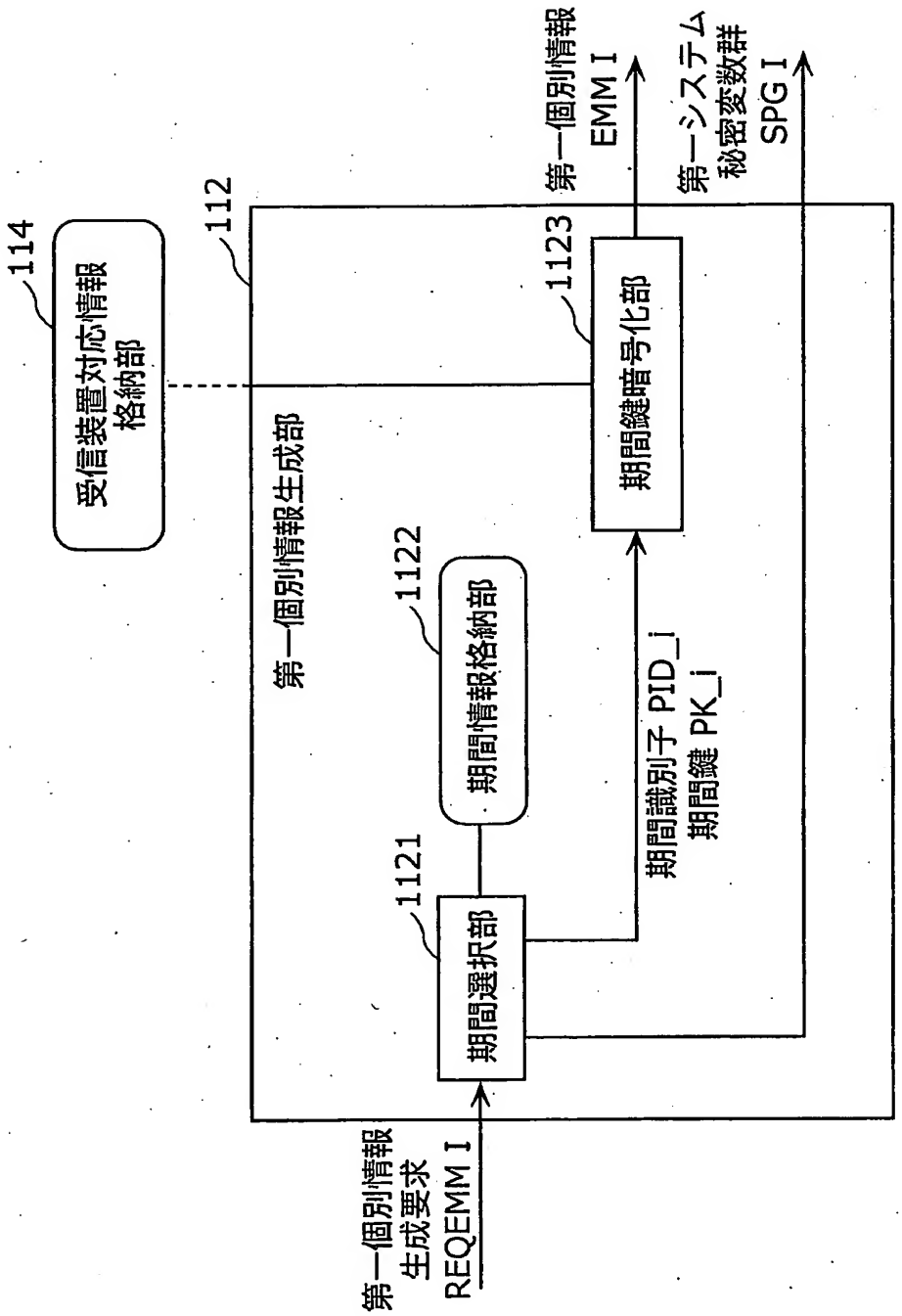


差替え用紙(規則26)

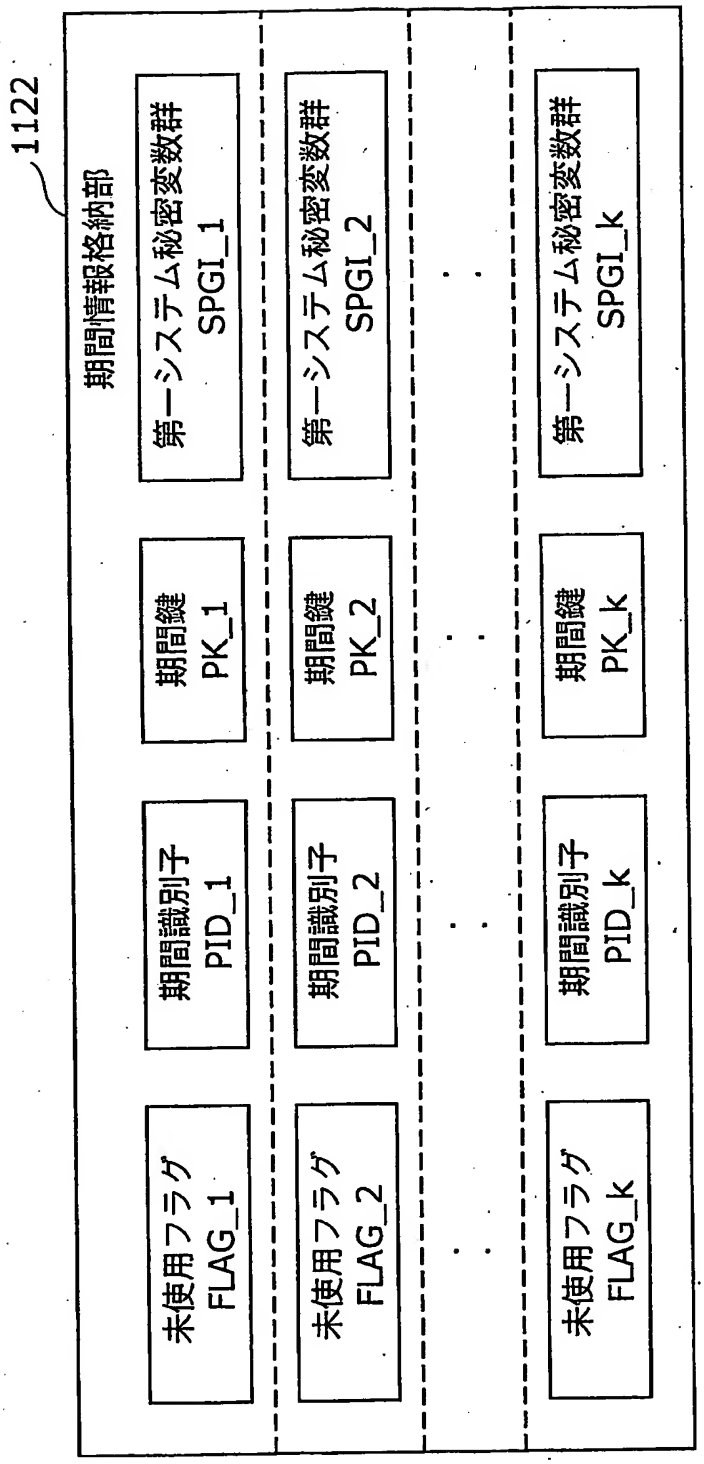
【図2】


11
鍵発行センタ
111
第一制御部
112
第一個別情報
生成要求
REQEMM I
第一個別情報
EMM I
113
受信装置
対応情報格納部
114
第二個別情報
生成要求
REQEMM II
第二個別情報
EMM II
第二システム
秘密鍵群
SPG II
116
個別情報群配信部
個別情報群
EMMG
115
システム秘密変数群集合
送信部
システム秘密
変数群集合
SPGS
第一システム秘密変数群
SPG I

【図3】

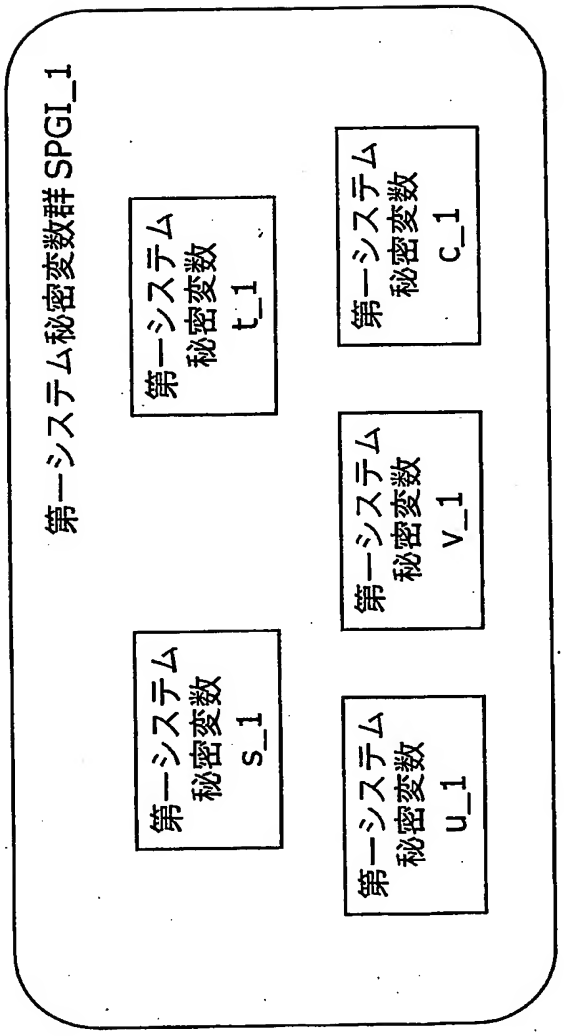

第一個別情報
生成要求
REQEMM I
第一個別情報生成部
112
受信装置対応情報
格納部
114
期間選択部
1121
期間情報格納部
1122
期間鍵暗号化部
1123
期間識別子 PID_i
期間鍵 PK_i
第一個別情報
EMM I
第一システム
秘密変数群
SPG I

【図4】

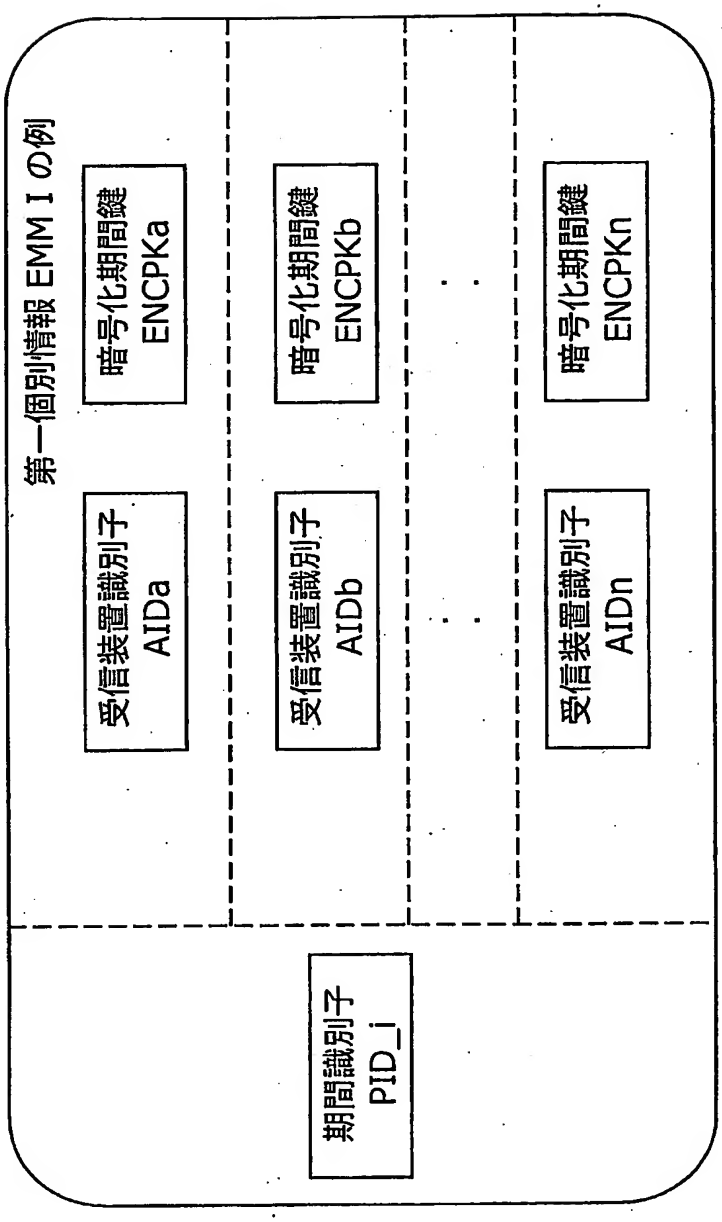


差替え用紙(規則26)

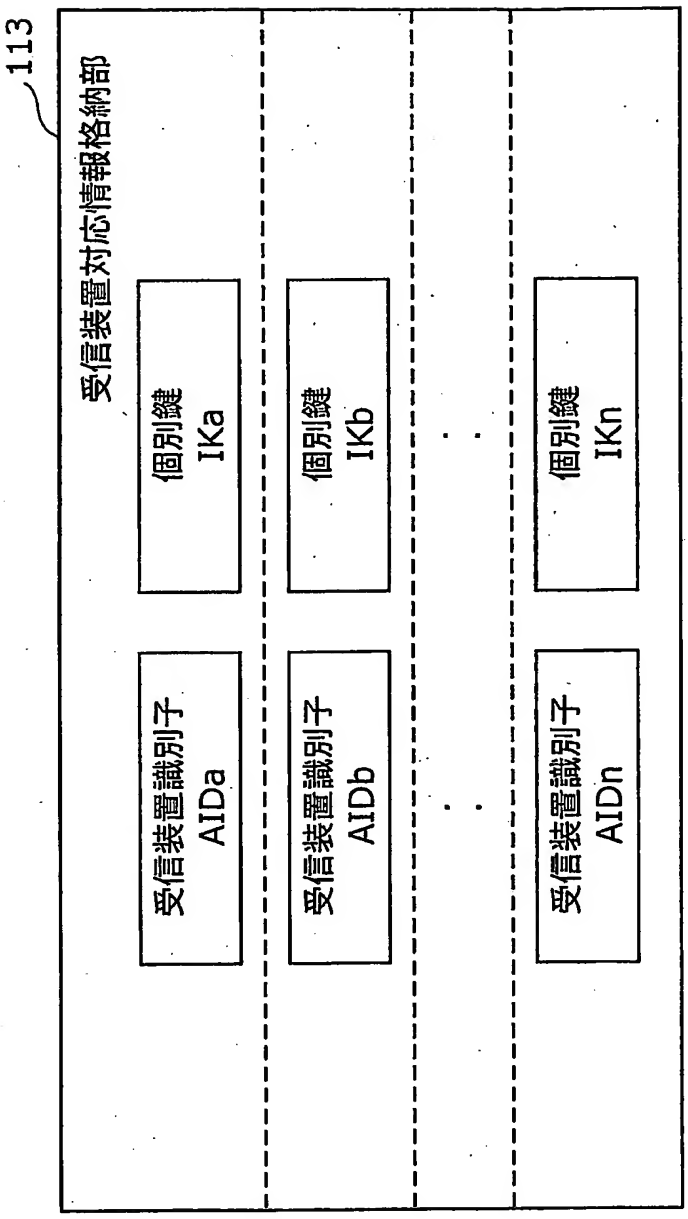
【図5】



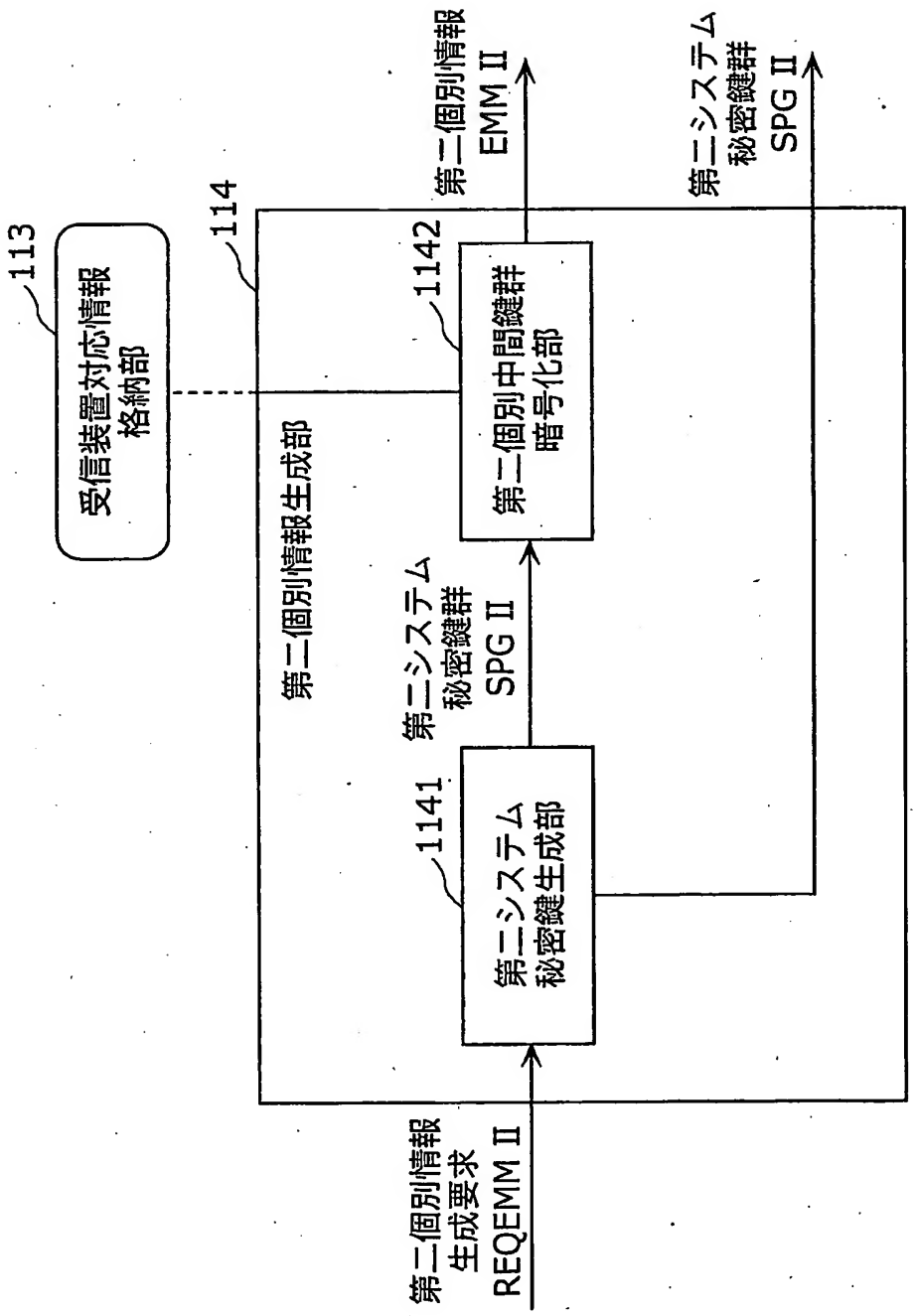
【図6】


第一個別情報 EMM I の例
暗号化期間鍵 ENCPKa
暗号化期間鍵 ENCPKb
暗号化期間鍵 ENCPKn
受信装置識別子 AIDa
受信装置識別子 AIDb
受信装置識別子 AIDn
期間識別子 PID_i

【図7】

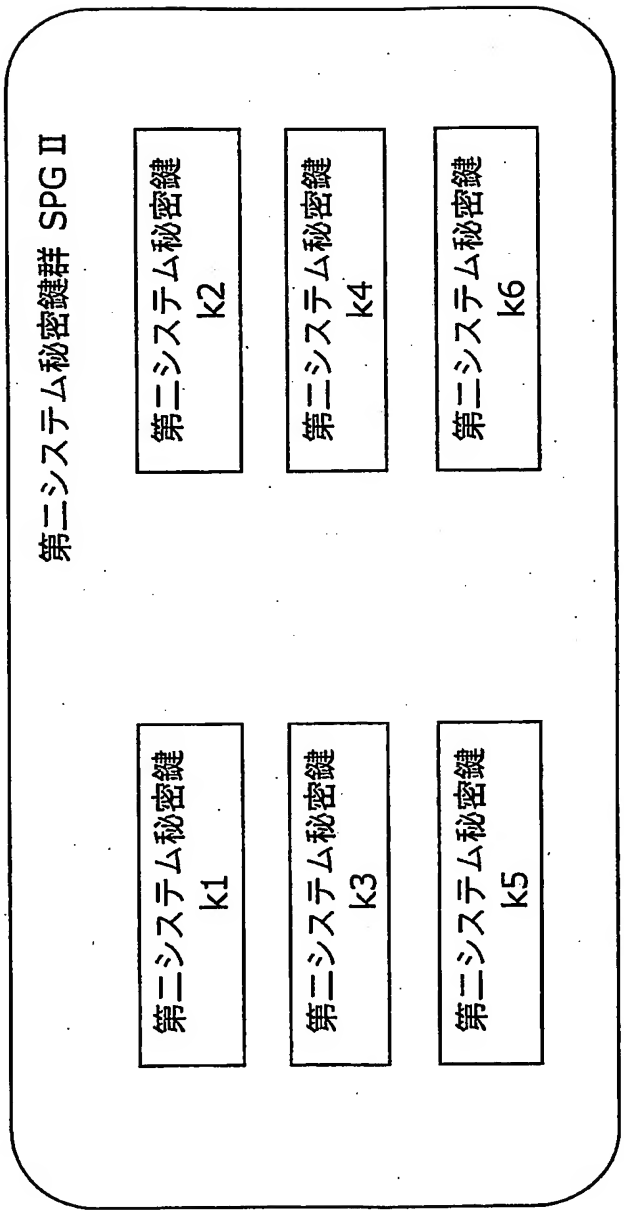

113
受信装置対応情報格納部
受信装置識別子 AIDa
個別鍵 IKa
受信装置識別子 AIDb
個別鍵 IKb
受信装置識別子 AIDn
個別鍵 IKn

【図8】

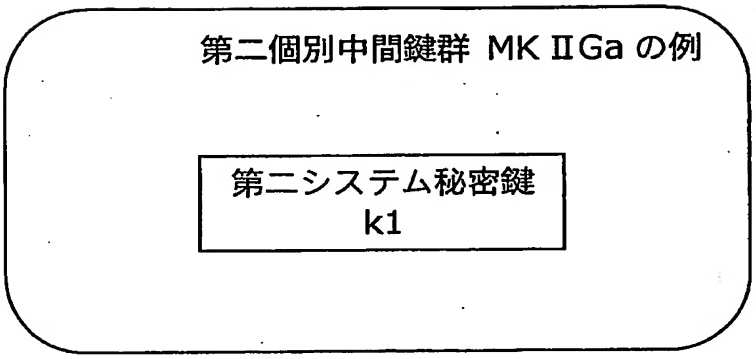


差替え用紙（規則26）

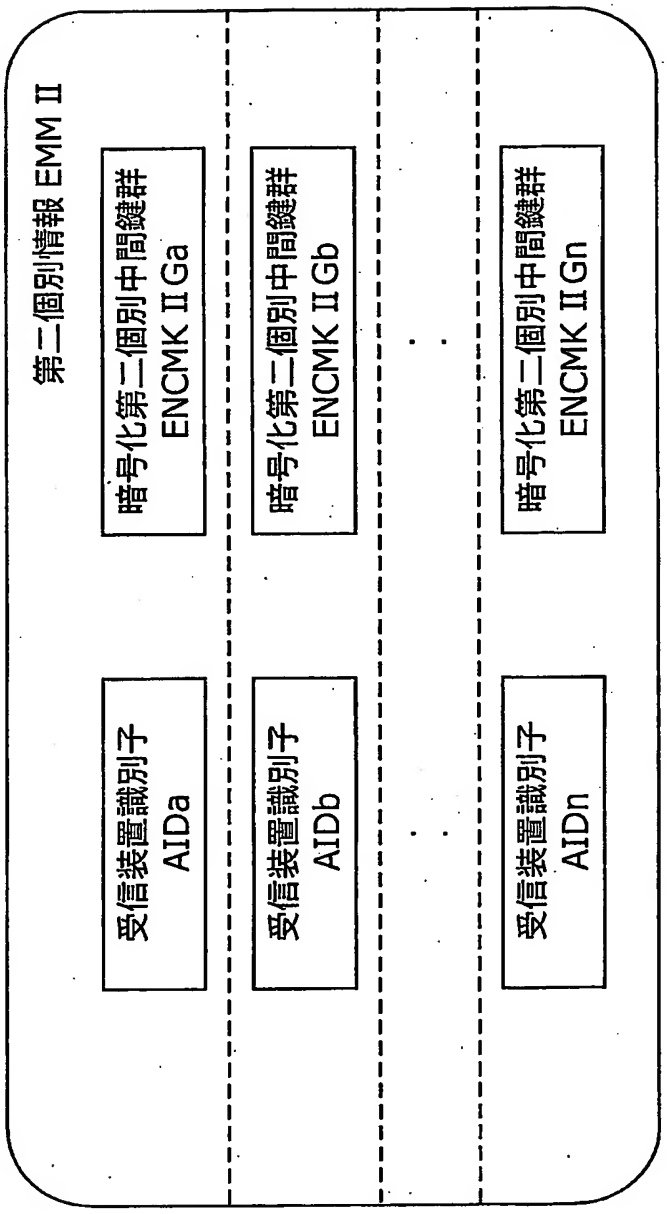
【図9】


第二システム秘密鍵群 SPG II
第二システム秘密鍵 k2
第二システム秘密鍵 k4
第二システム秘密鍵 k6
第二システム秘密鍵 k1
第二システム秘密鍵 k3
第二システム秘密鍵 k5

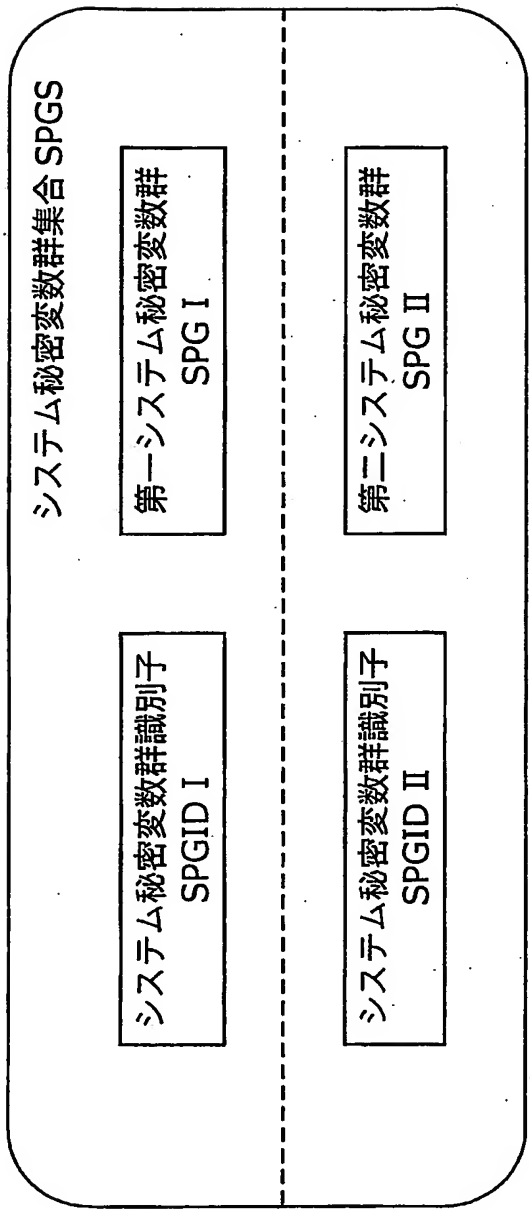
【図10】



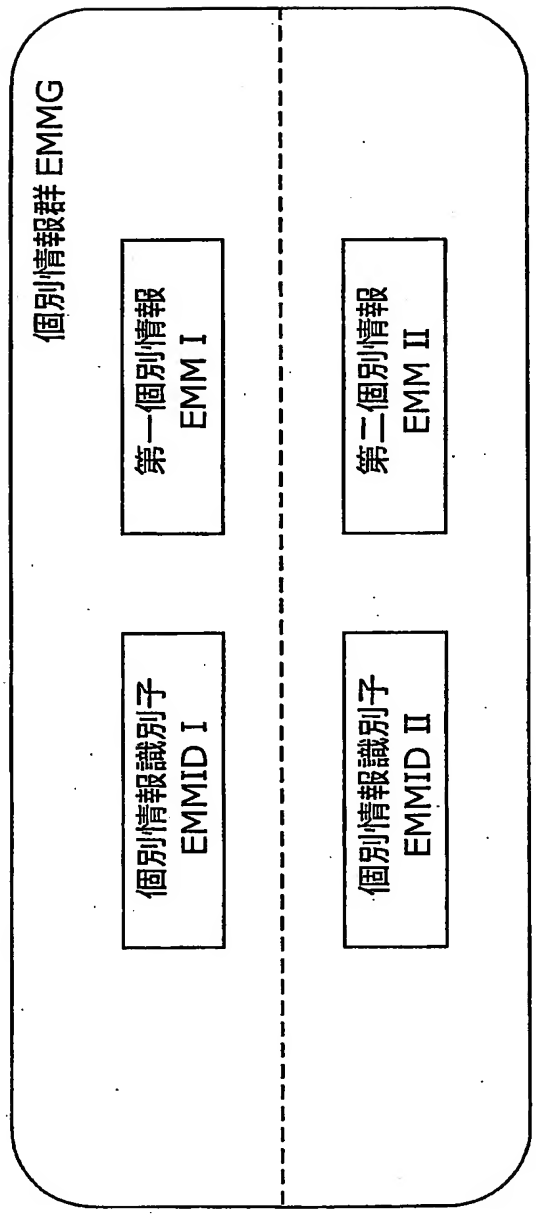
【図11】


第二個別情報 EMM II
暗号化第二個別中間鍵群 ENCMK IIGa
暗号化第二個別中間鍵群 ENCMK IIGb
暗号化第二個別中間鍵群 ENCMK IIGn
受信装置識別子 AIDa
受信装置識別子 AIDb
受信装置識別子 AIDn

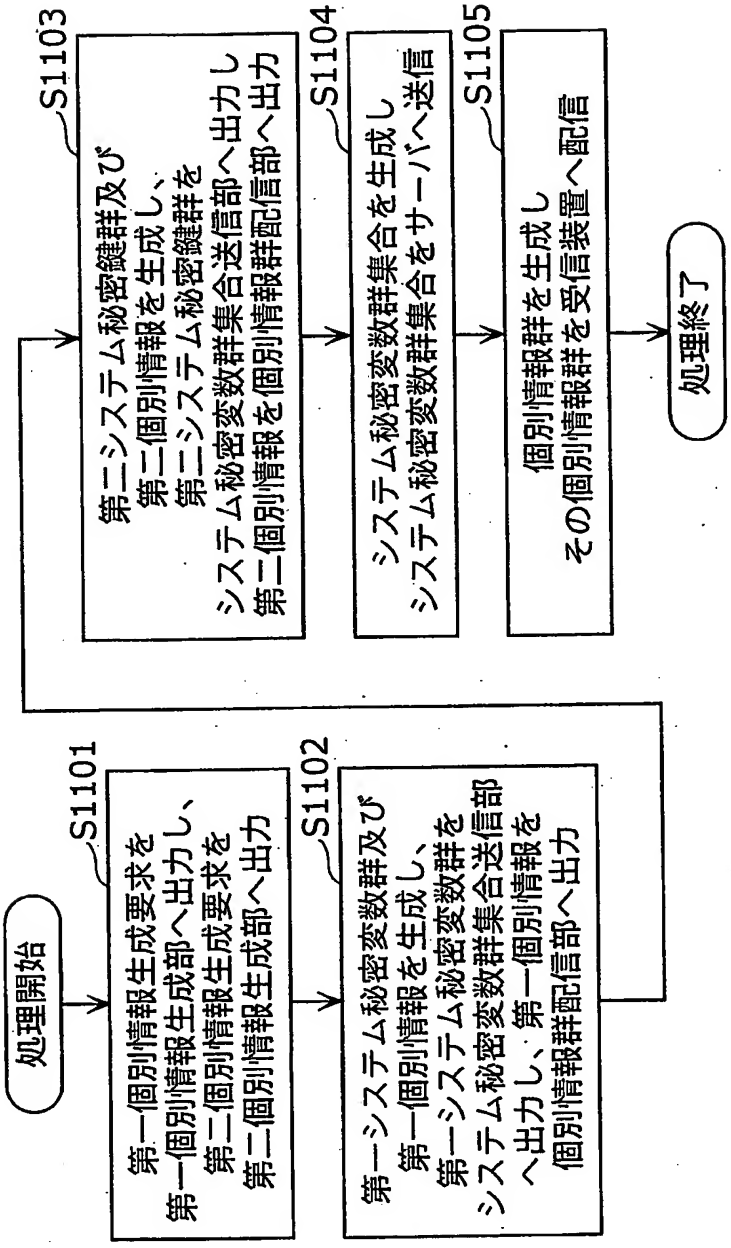
【図12】


システム秘密変数群集合 SPGS
第一システム秘密変数群
SPG I
第二システム秘密変数群
SPG II
システム秘密変数群識別子
SPGID I
システム秘密変数群識別子
SPGID II

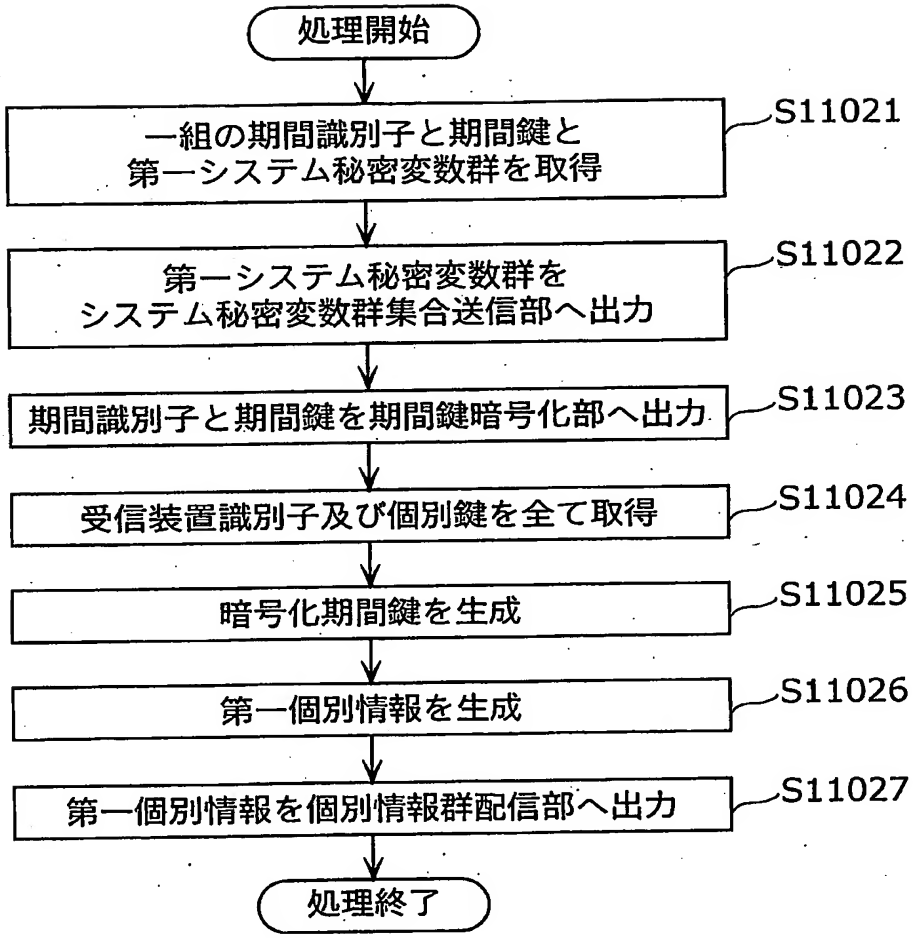
【図13】


個別情報群 EMMG
第一個別情報
EMM I
第二個別情報
EMM II
個別情報識別子
EMMID I
個別情報識別子
EMMID II

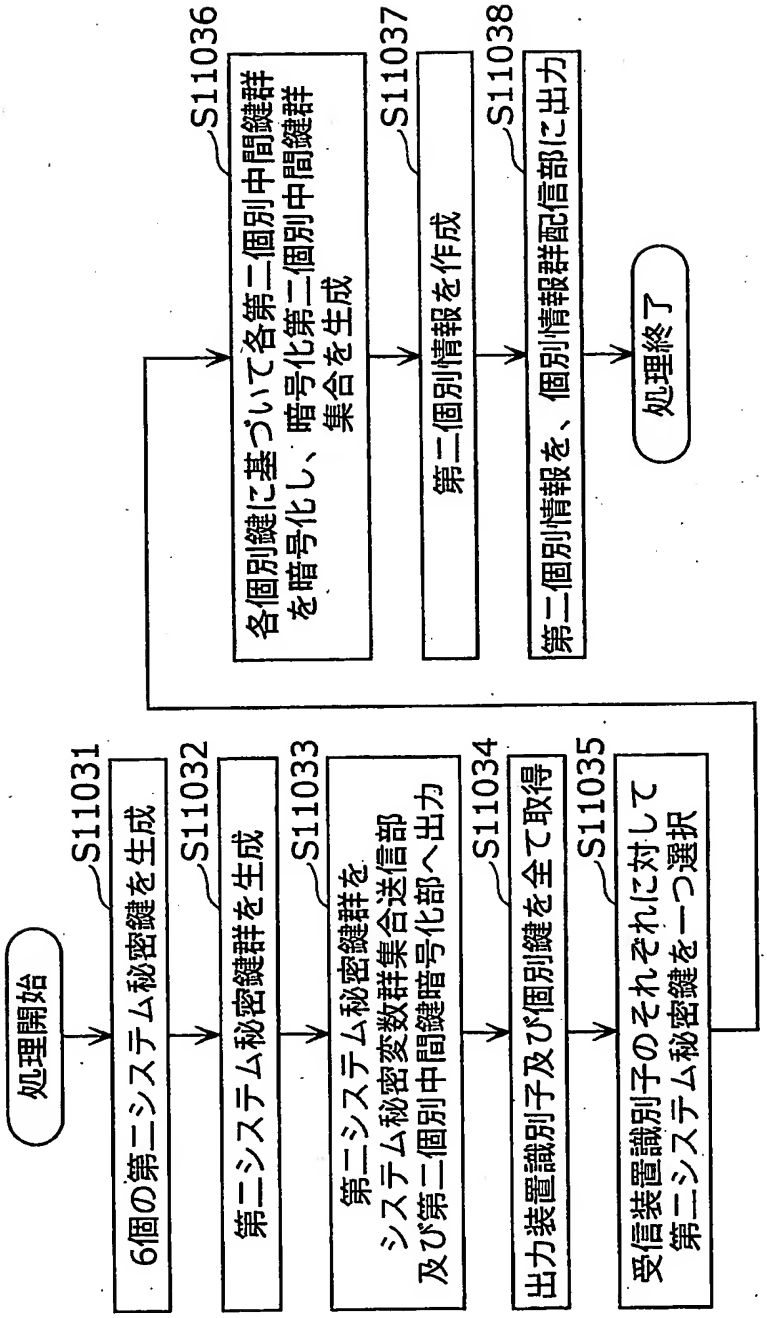
【図14】


処理開始
S1101
第一個別情報生成要求を
第一個別情報生成部へ出力し、
第二個別情報生成要求を
第二個別情報生成部へ出力
S1102
第一システム秘密変数群及び
第一個別情報を生成し、
第一システム秘密変数群を
システム秘密変数群集合送信部
へ出力し、第一個別情報を
個別情報群配信部へ出力
S1103
第二システム秘密鍵群及び
第二個別情報を生成し、
第二システム秘密鍵群を
システム秘密変数群集合送信部へ出力し
第二個別情報を個別情報群配信部へ出力
S1104
システム秘密変数群集合を生成し
システム秘密変数群集合をサーバへ送信
S1105
個別情報群を生成し
その個別情報群を受信装置へ配信
処理終了

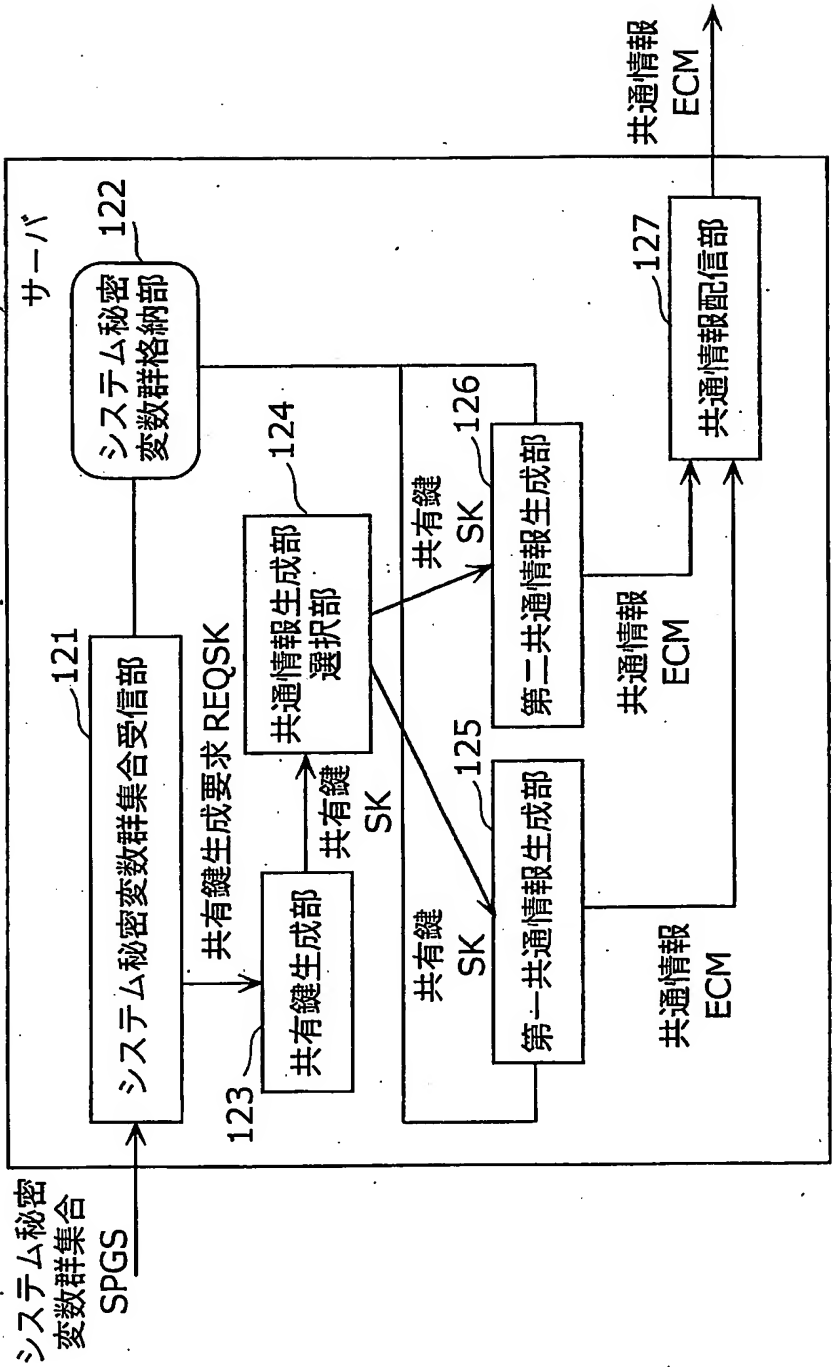
【図15】


処理開始
一組の期間識別子と期間鍵と
第一システム秘密変数群を取得
S11021
第一システム秘密変数群を
システム秘密変数群集合送信部へ出力
S11022
期間識別子と期間鍵を期間鍵暗号化部へ出力
S11023
受信装置識別子及び個別鍵を全て取得
S11024
暗号化期間鍵を生成
S11025
第一個別情報を生成
S11026
第一個別情報を個別情報群配信部へ出力
S11027
処理終了

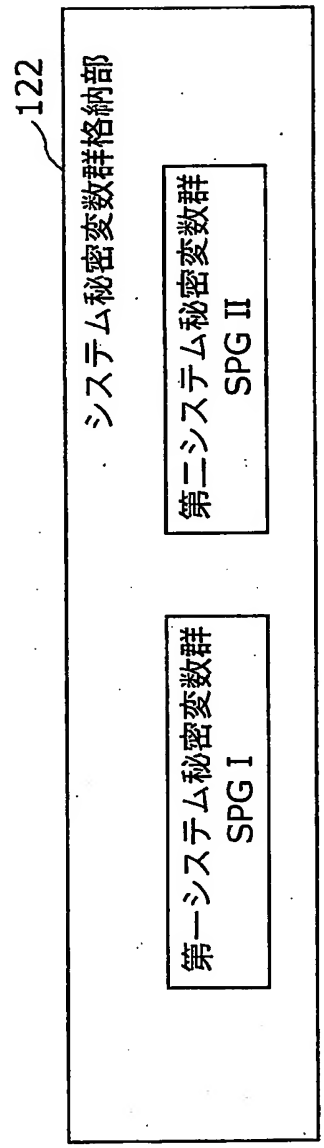
【図16】


処理開始
S11031
6個の第二システム秘密鍵を生成
S11032
第二システム秘密鍵群を生成
S11033
第二システム秘密鍵群を
システム秘密変数群集合送信部
及び第二個別中間鍵暗号化部へ出力
S11034
出力装置識別子及び個別鍵を全て取得
S11035
受信装置識別子のそれぞれに対して
第二システム秘密鍵を一つ選択
S11036
各個別鍵に基づいて各第二個別中間鍵群
を暗号化し、暗号化第二個別中間鍵群
集合を生成
S11037
第二個別情報を作成
S11038
第二個別情報を、個別情報群配信部に出力
処理終了

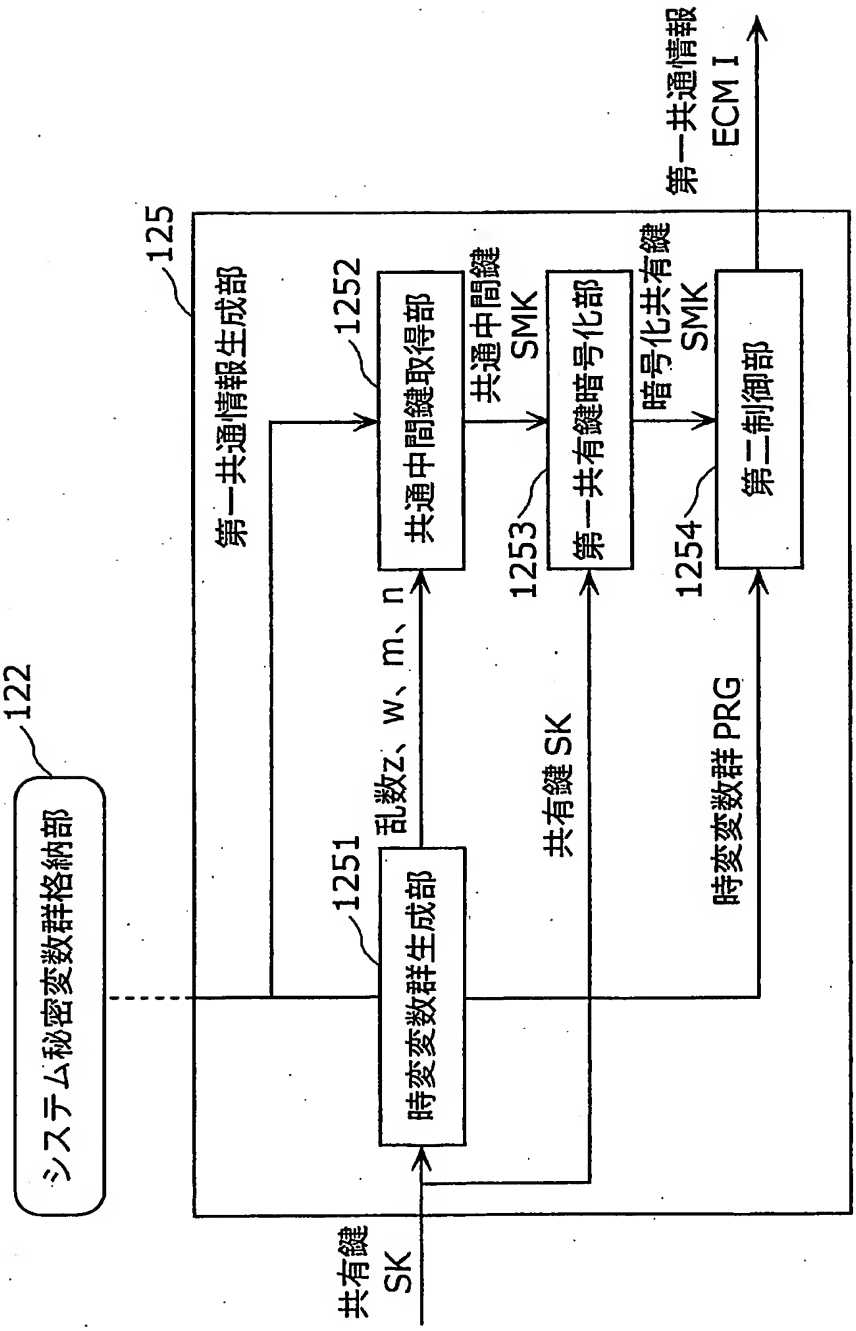
【図17】


12
サーバ
121
システム秘密変数群集合受信部
122
システム秘密変数群格納部
123
共有鍵生成部
124
共通情報生成部選択部
125
第一共通情報生成部
126
第二共通情報生成部
127
共通情報配信部
システム秘密変数群集合 SPGS
共有鍵生成要求 REQSK
共有鍵 SK
共有鍵 SK
共有鍵 SK
共通情報 ECM
共通情報 ECM
共通情報 ECM

【図18】

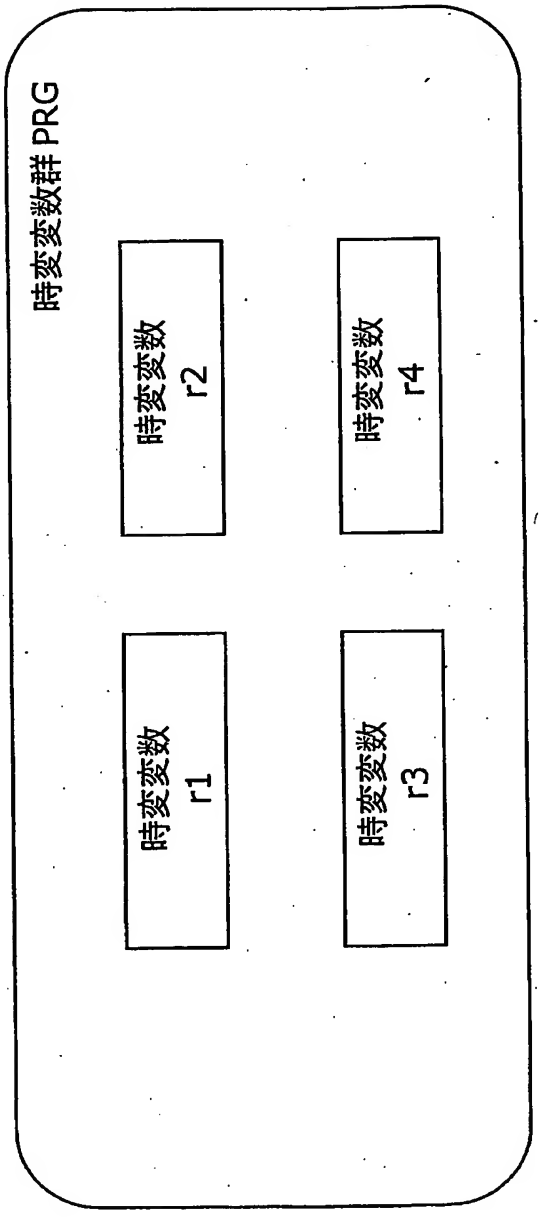


【図19】

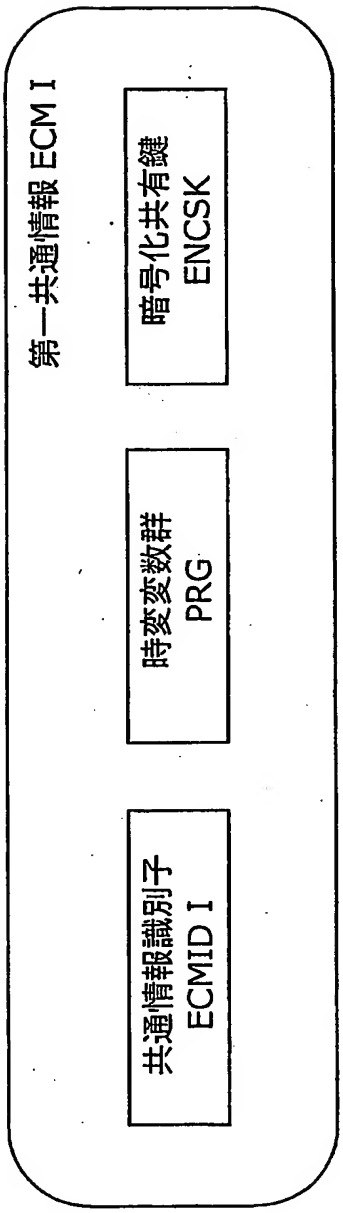


差替え用紙（規則26）

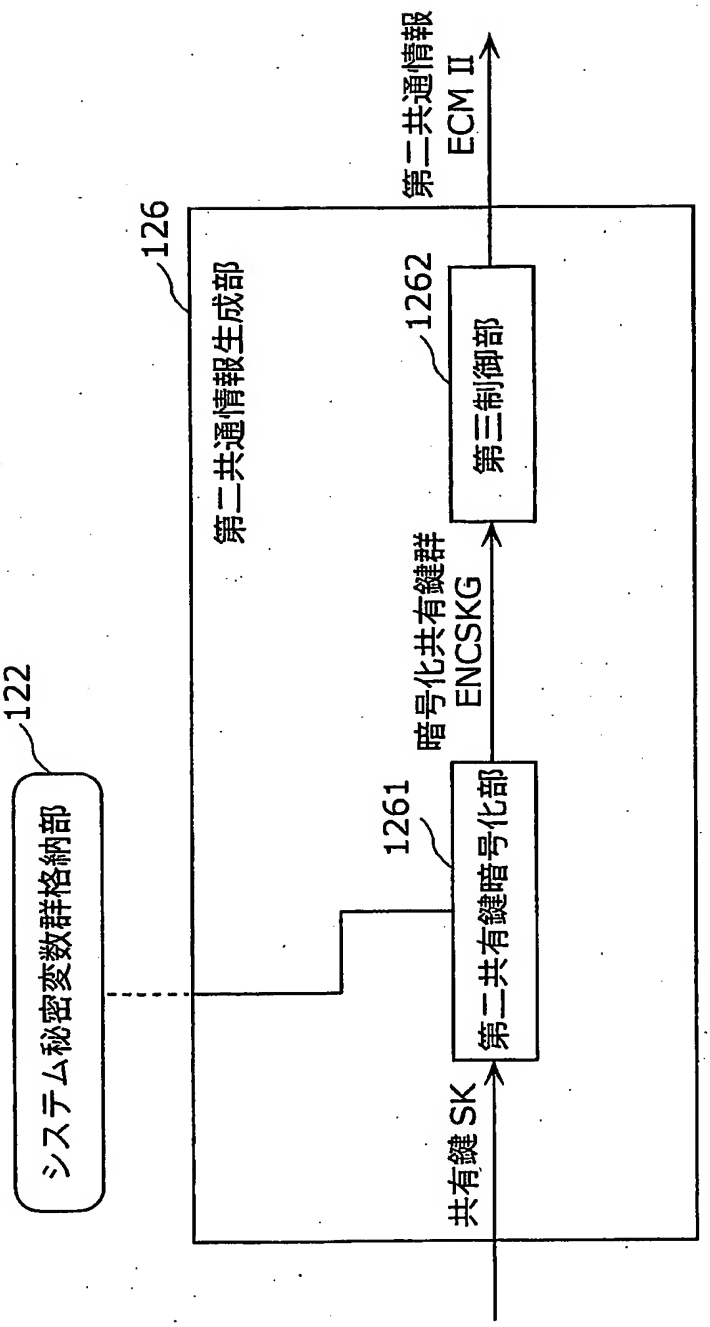
【図20】



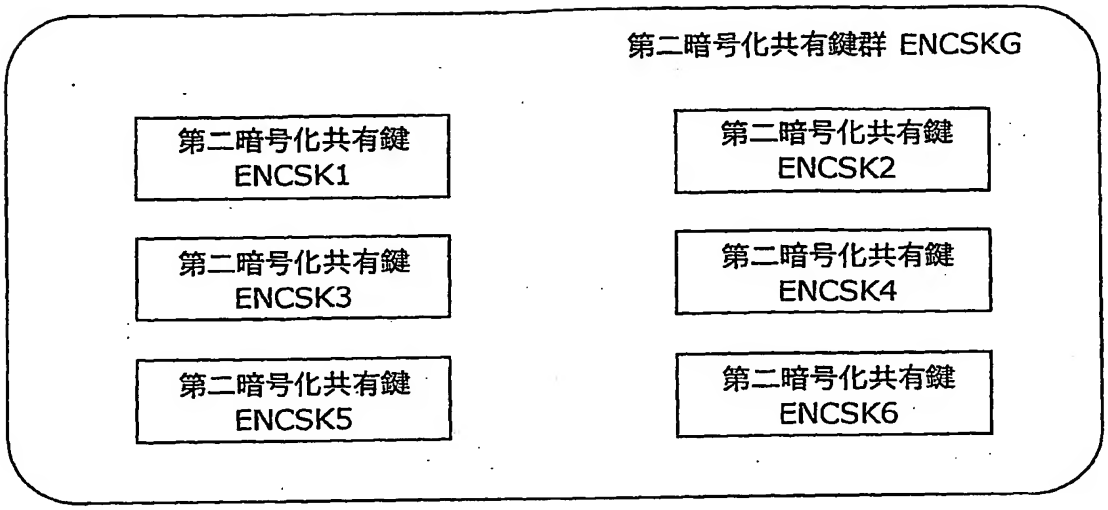
【図21】



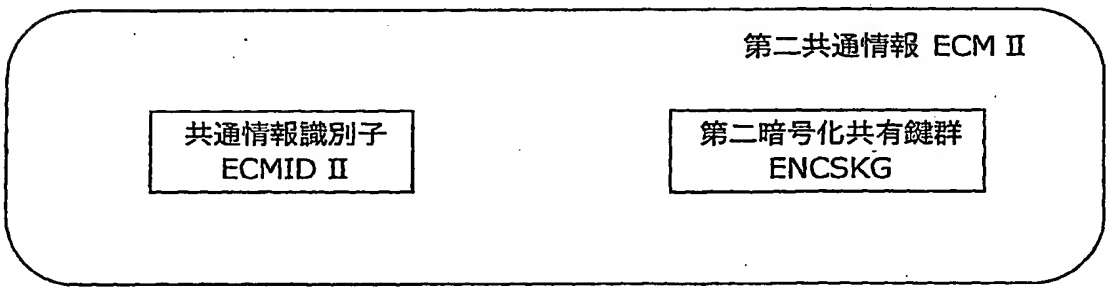
【図22】


122
システム秘密変数群格納部
126
第二共通情報生成部
1261
第二共有鍵暗号化部
1262
第三制御部
暗号化共有鍵群
ENCSKG
第二共通情報
ECM II
共有鍵 SK

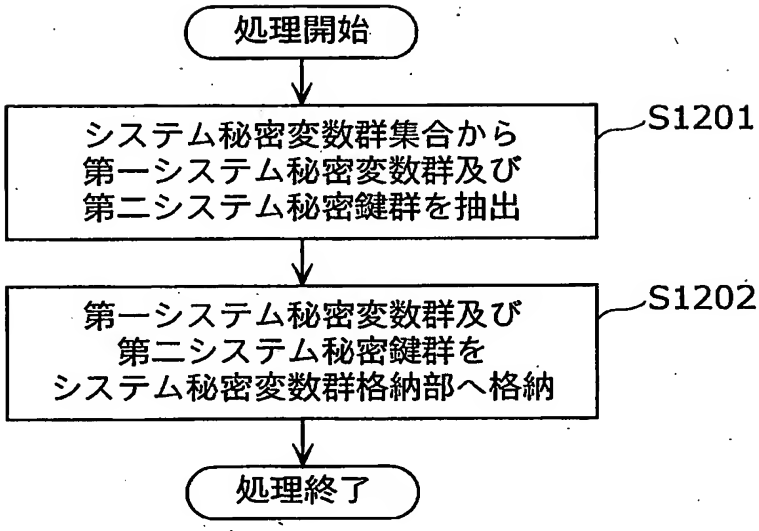
【図23】


第二暗号化共有鍵群 ENCSKG
第二暗号化共有鍵 ENCSK1
第二暗号化共有鍵 ENCSK2
第二暗号化共有鍵 ENCSK3
第二暗号化共有鍵 ENCSK4
第二暗号化共有鍵 ENCSK5
第二暗号化共有鍵 ENCSK6

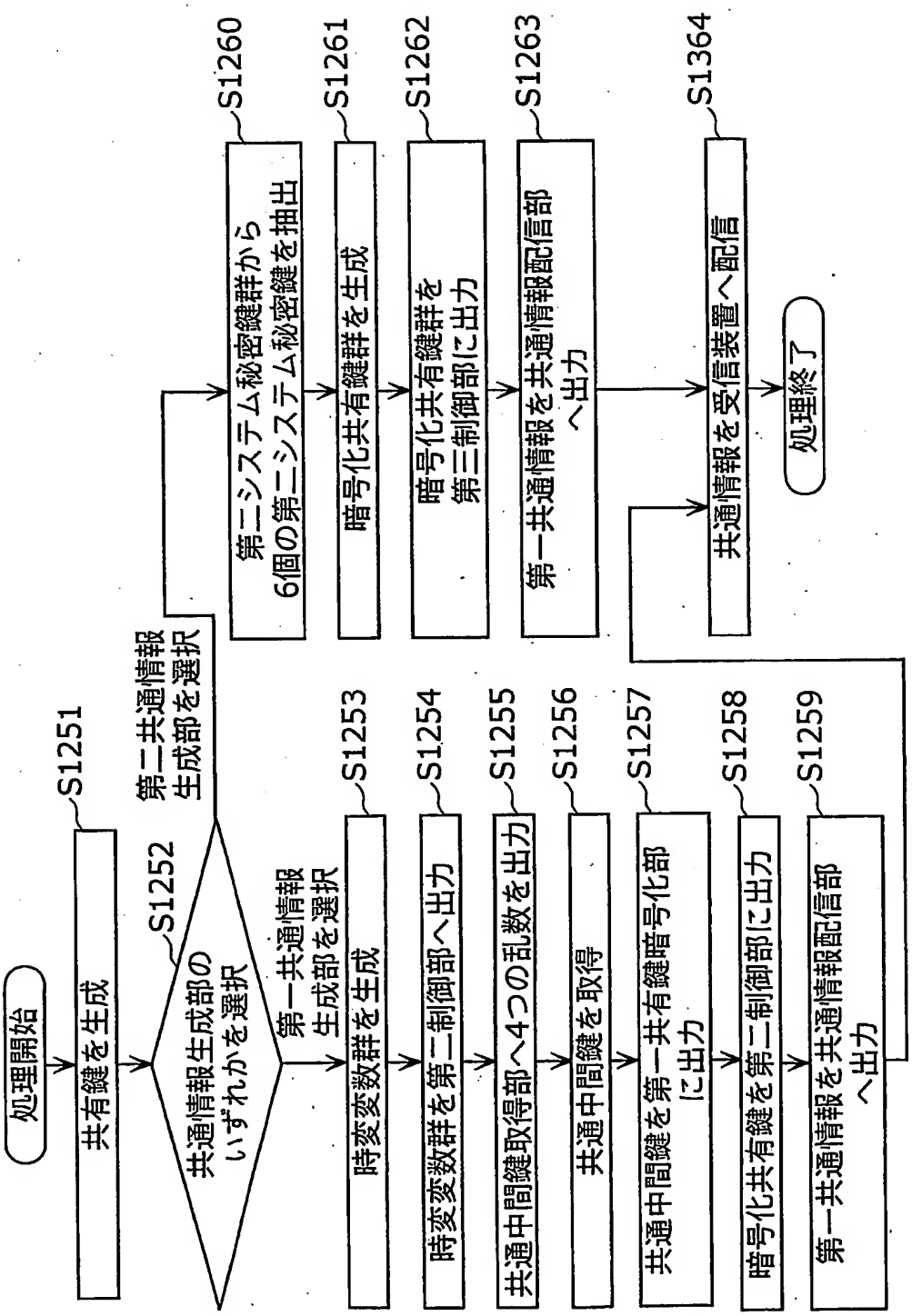
【図24】


第二共通情報 ECM II
共通情報識別子 ECMID II
第二暗号化共有鍵群 ENCSKG

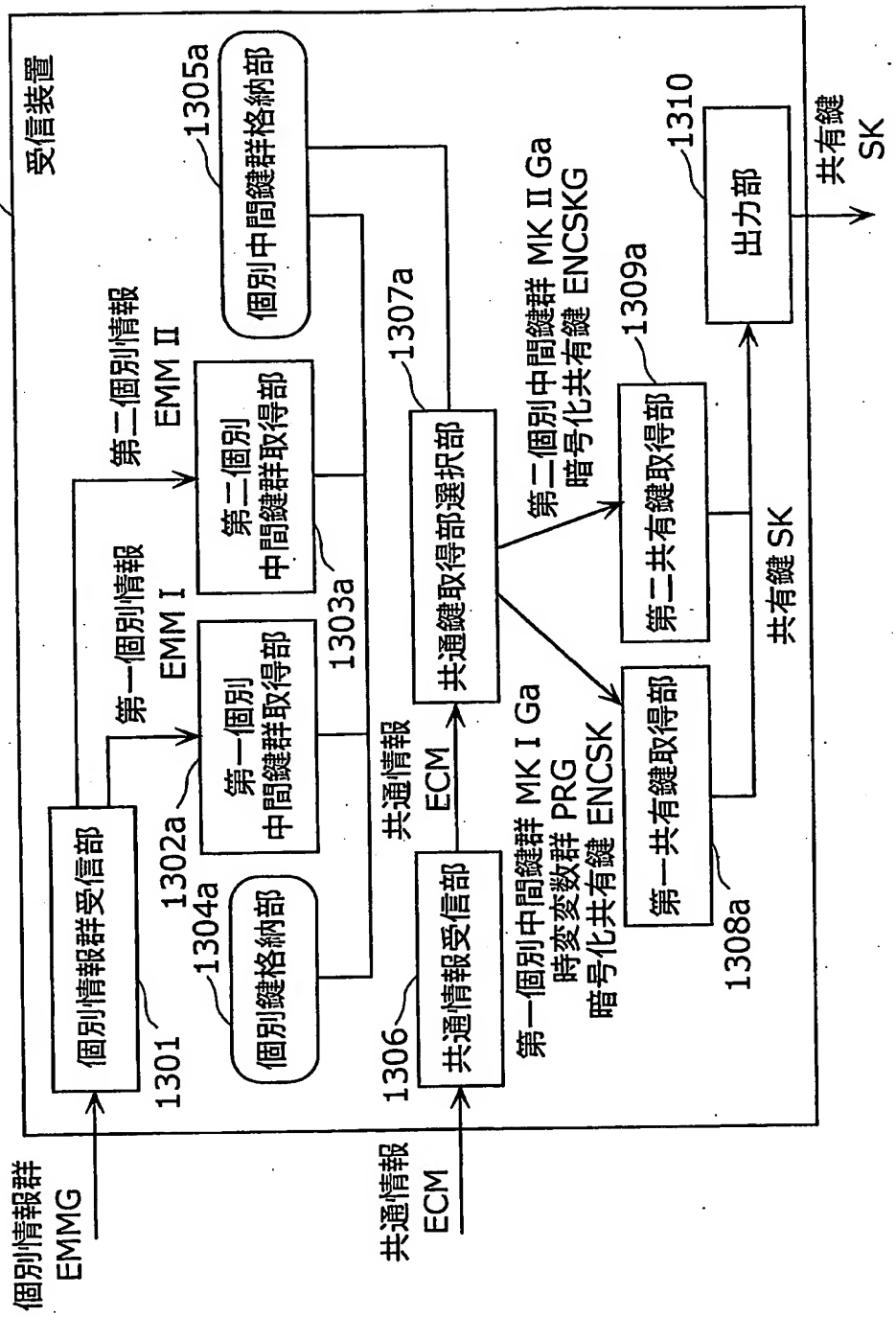
【図25】


処理開始
システム秘密変数群集合から
第一システム秘密変数群及び
第二システム秘密鍵群を抽出
S1201
第一システム秘密変数群及び
第二システム秘密鍵群を
システム秘密変数群格納部へ格納
S1202
処理終了

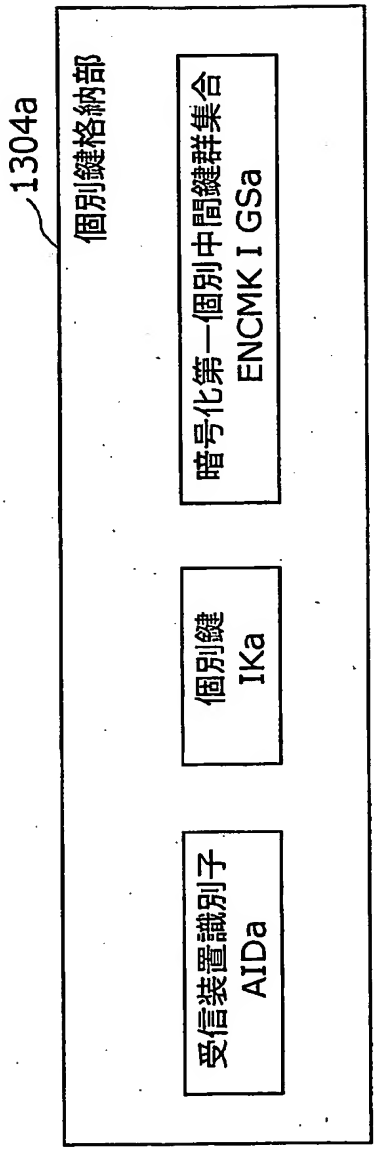
【図26】


処理開始
S1251
共有鍵を生成
S1252
共通情報生成部のいずれかを選択
第二共通情報生成部を選択
S1260
第二システム秘密鍵群から6個の第二システム秘密鍵を抽出
S1261
暗号化共有鍵群を生成
S1262
暗号化共有鍵群を第三制御部に出力
S1263
第一共通情報を共通情報配信部へ出力
S1364
共通情報を受信装置へ配信
処理終了
第一共通情報生成部を選択
S1253
時変変数群を生成
S1254
時変変数群を第二制御部へ出力
S1255
共通中間鍵取得部へ4つの乱数を出力
S1256
共通中間鍵を取得
S1257
共通中間鍵を第一共有鍵暗号化部に出力
S1258
暗号化共有鍵を第二制御部に出力
S1259
第一共通情報を共通情報配信部へ出力

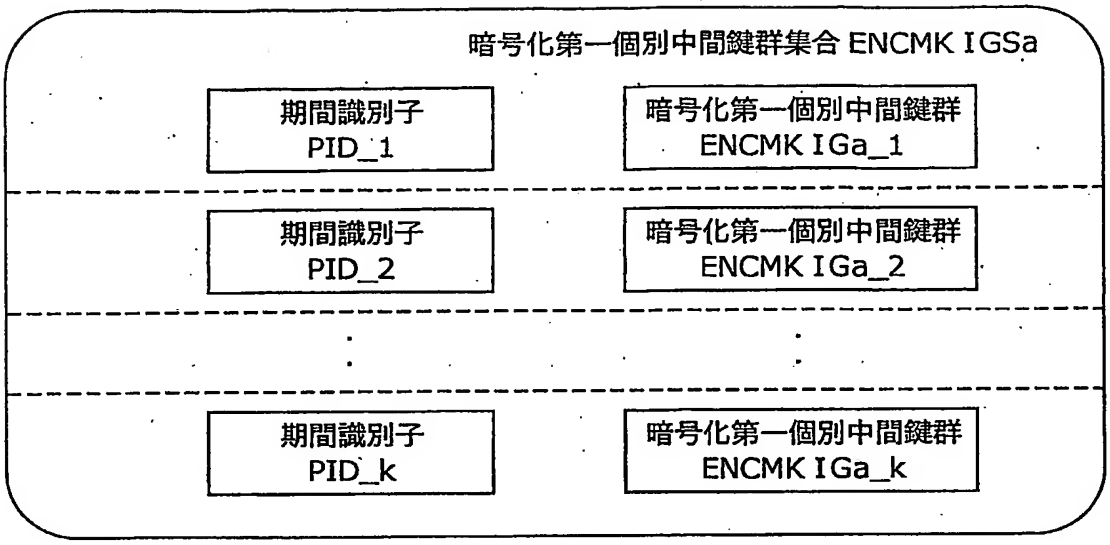
【図27】


13a
受信装置
個別情報群 EMMG
個別情報群受信部
1301
第一個別情報 EMM I
第二個別情報 EMM II
1302a
第一個別中間鍵群取得部
第二個別中間鍵群取得部
1303a
1304a
個別鍵格納部
1305a
個別中間鍵群格納部
共通情報 ECM
共通情報受信部
1306
共通鍵取得部選択部
1307a
第一個別中間鍵群 MK I Ga
時変変数群 PRG
暗号化共有鍵 ENCSK
第二個別中間鍵群 MK II Ga
暗号化共有鍵 ENCSKG
第一共有鍵取得部
1308a
第二共有鍵取得部
1309a
出力部
1310
共有鍵 SK
共有鍵 SK

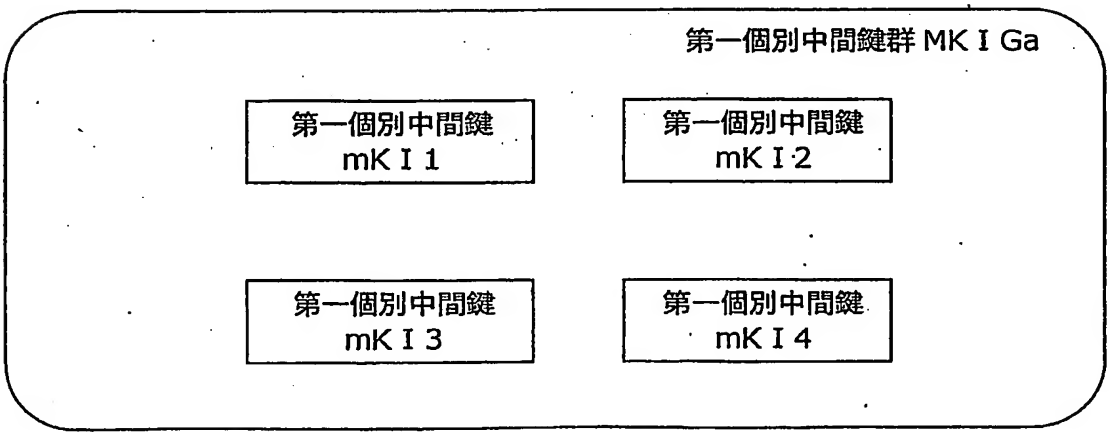
【図28】


1304a
個別鍵格納部
暗号化第一個別中間鍵群集合
ENCMK I GSa
個別鍵
IKa
受信装置識別子
AIDa

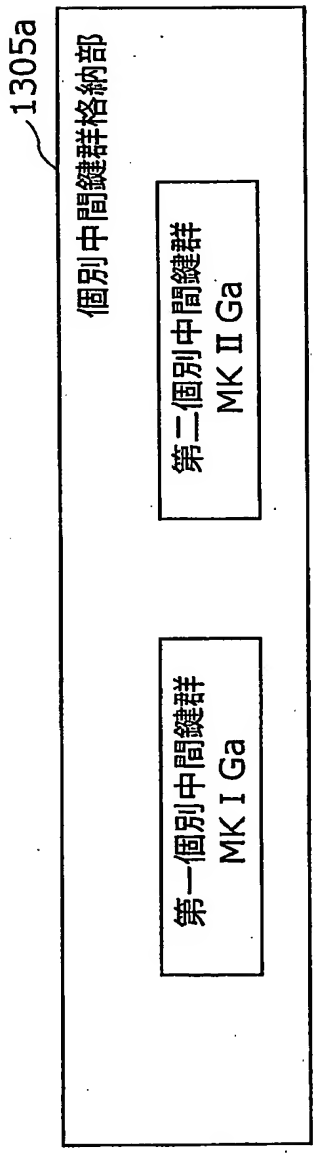
【図29】


暗号化第一個別中間鍵群集合 ENCMK IGSa
期間識別子 PID_1
暗号化第一個別中間鍵群 ENCMK IGa_1
期間識別子 PID_2
暗号化第一個別中間鍵群 ENCMK IGa_2
期間識別子 PID_k
暗号化第一個別中間鍵群 ENCMK IGa_k

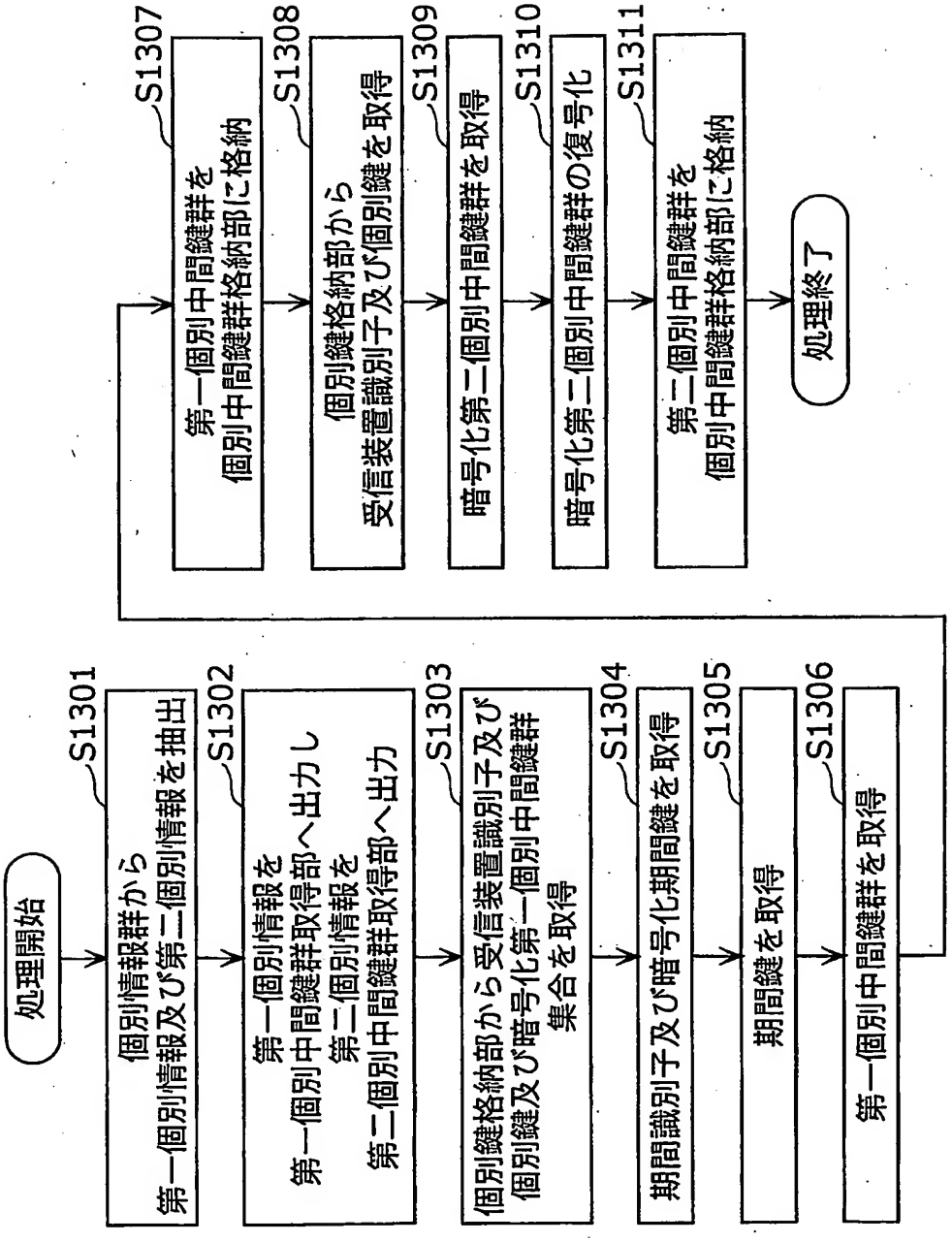
【図30】


第一個別中間鍵群 MK I Ga
第一個別中間鍵 mK I 1
第一個別中間鍵 mK I 2
第一個別中間鍵 mK I 3
第一個別中間鍵 mK I 4

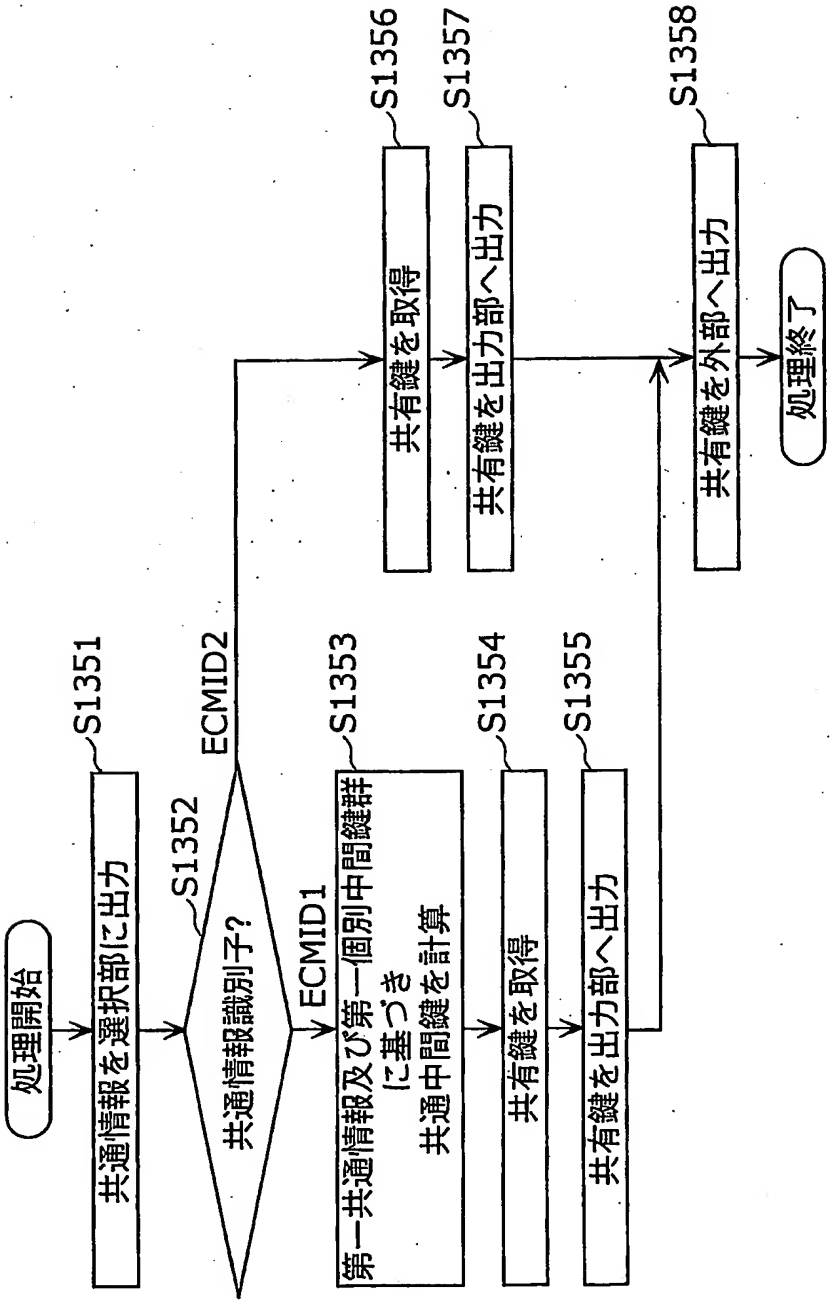
【図31】



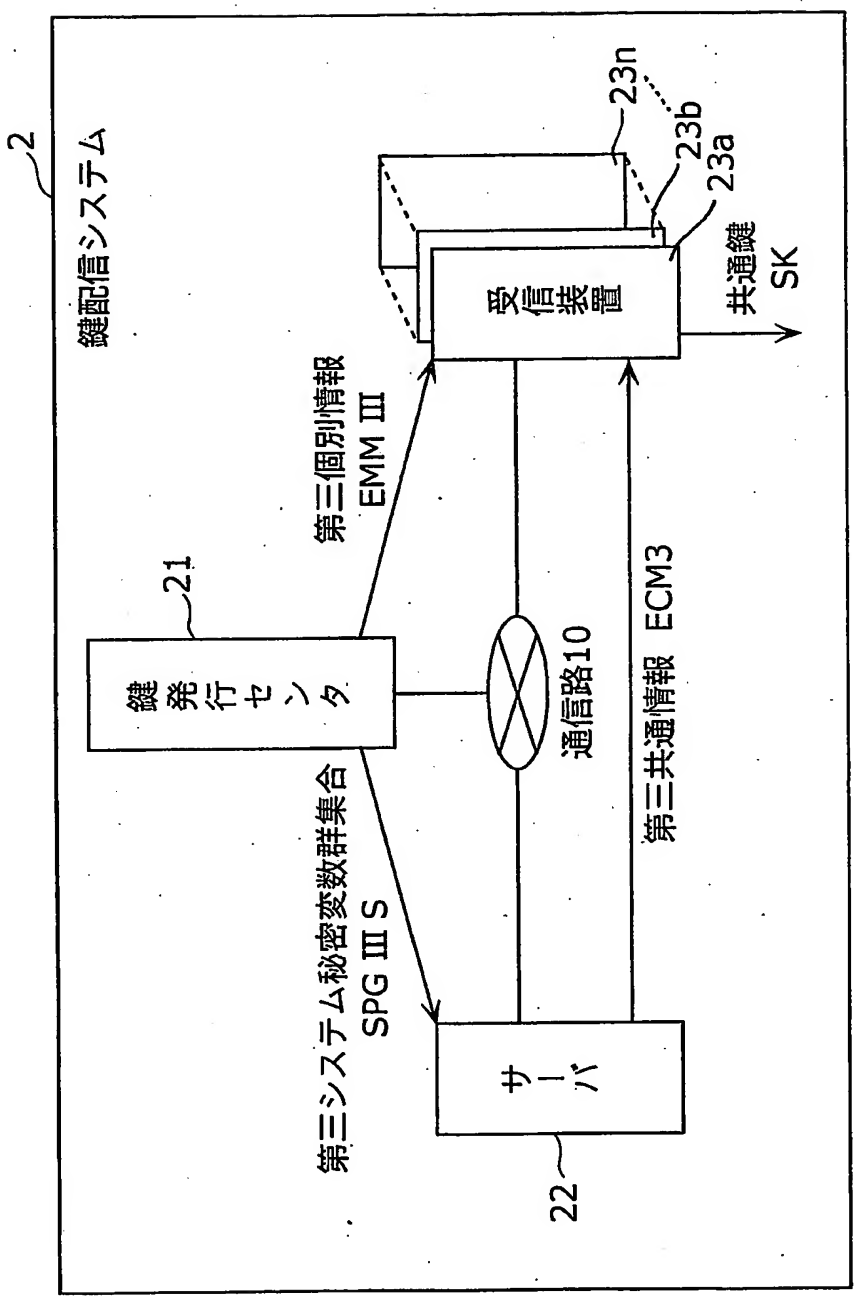
【図32】



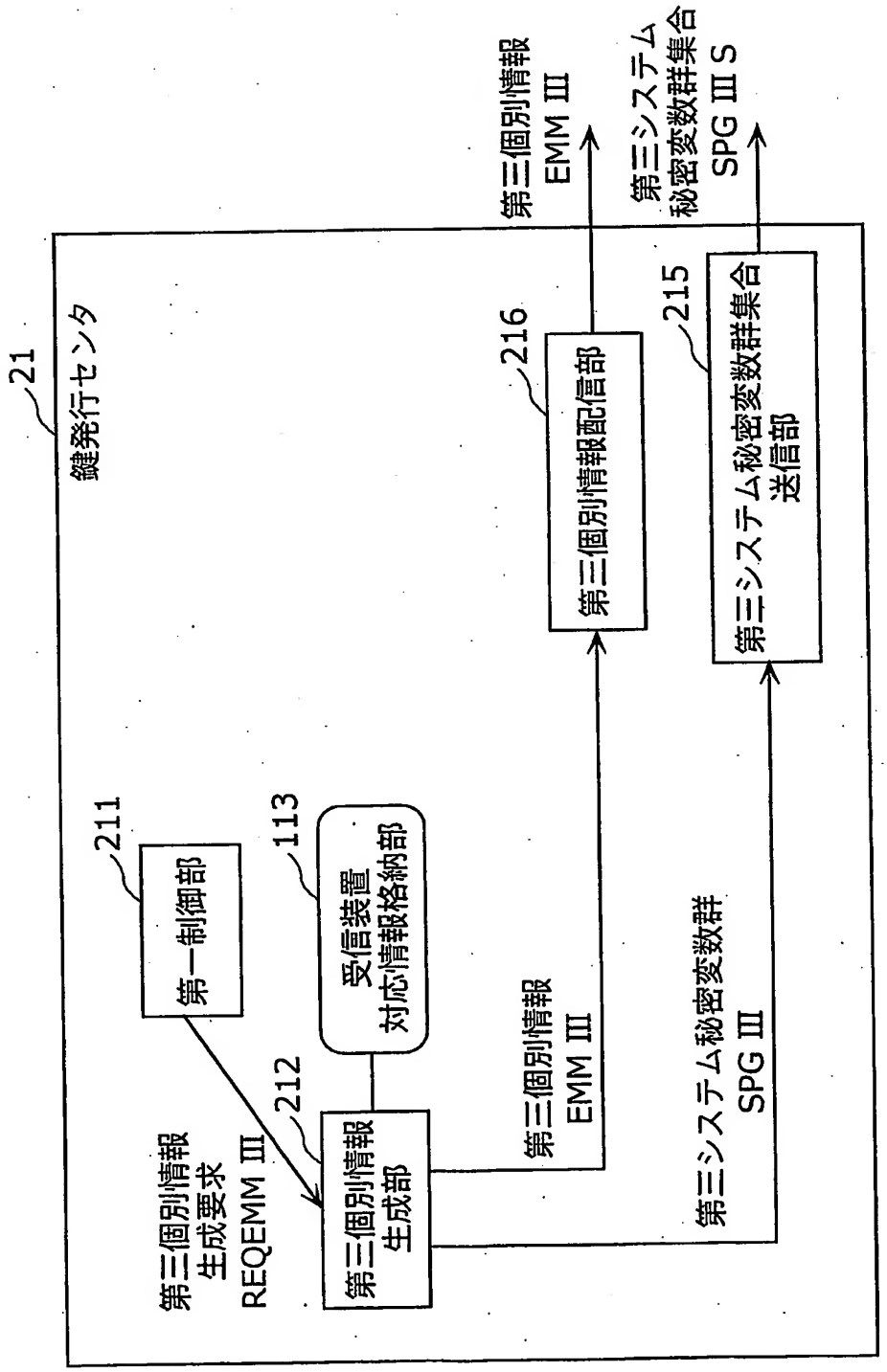
【図33】


処理開始
S1351
共通情報を選択部に出力
S1352
共通情報識別子?
ECMID2
ECMID1
S1353
第一共通情報及び第一個別中間鍵群
に基づき
共通中間鍵を計算
S1354
共有鍵を取得
S1355
共有鍵を出力部へ出力
S1356
共有鍵を取得
S1357
共有鍵を出力部へ出力
S1358
共有鍵を外部へ出力
処理終了

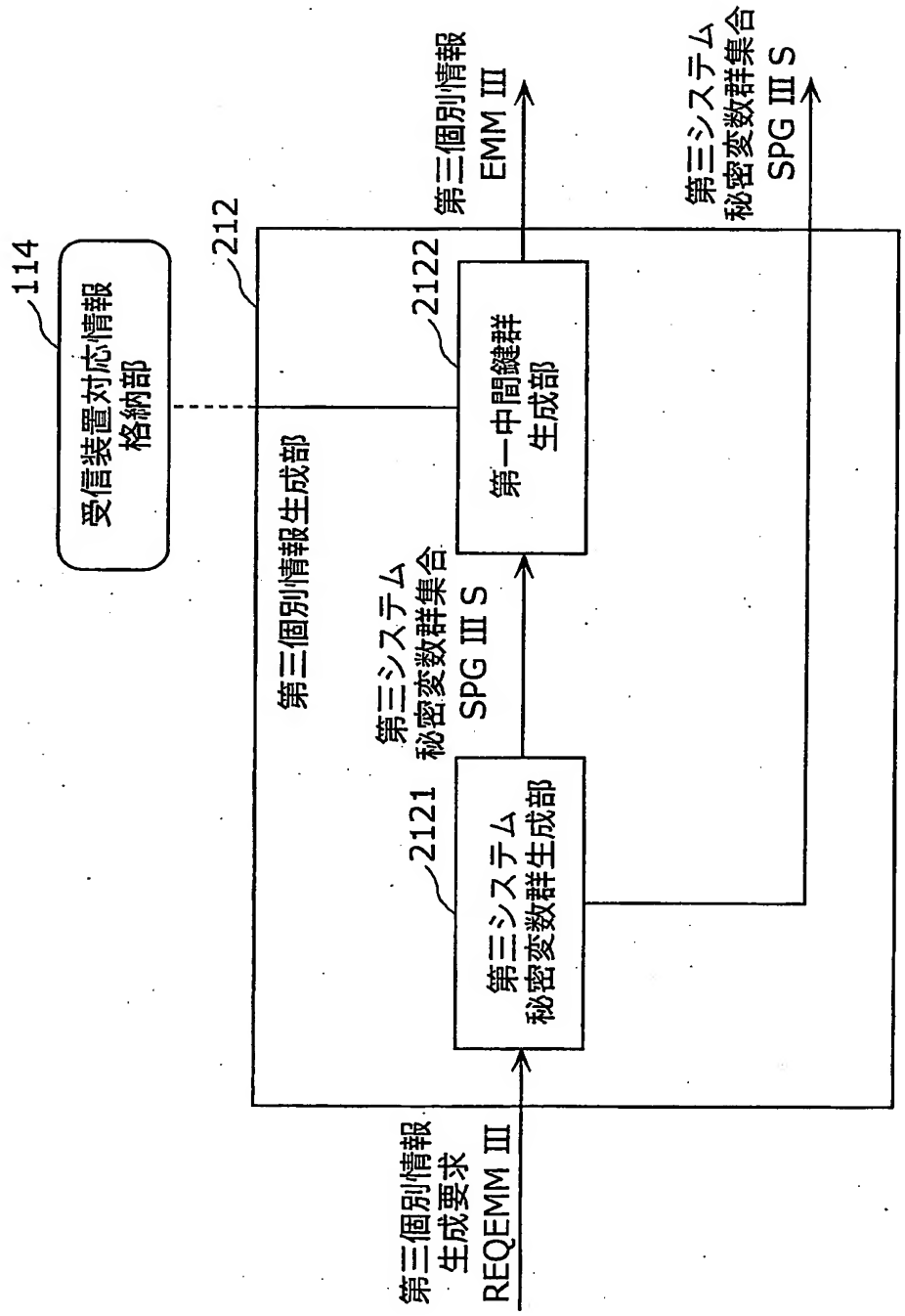
【図34】



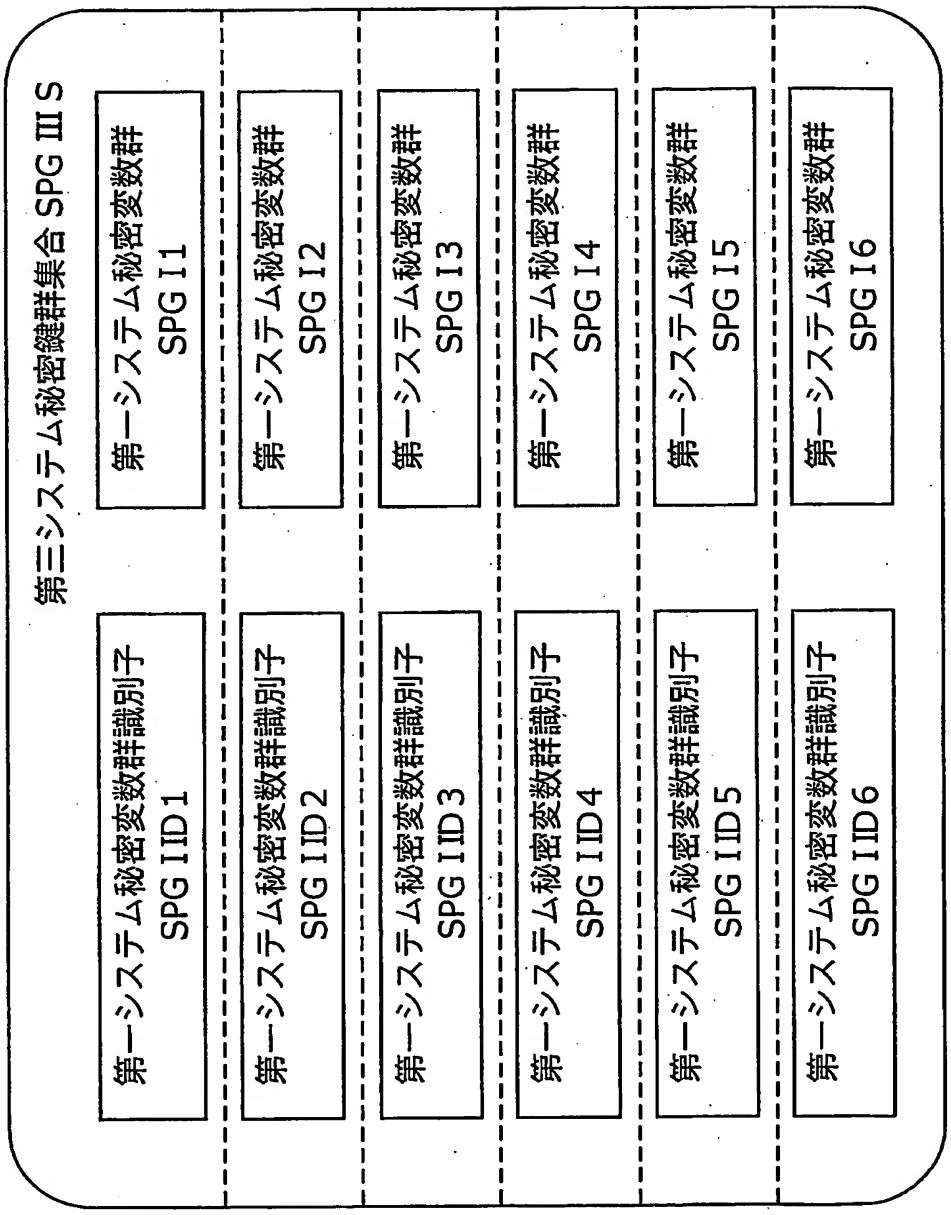
【図35】


21
鍵発行センタ
211
第一制御部
113
受信装置
対応情報格納部
212
第三個別情報
生成部
第三個別情報
生成要求
REQEMM III
216
第三個別情報配信部
215
第三システム秘密変数群集合
送信部
第三個別情報
EMM III
第三システム
秘密変数群集合
SPG III S
第三個別情報
EMM III
第三システム秘密変数群
SPG III

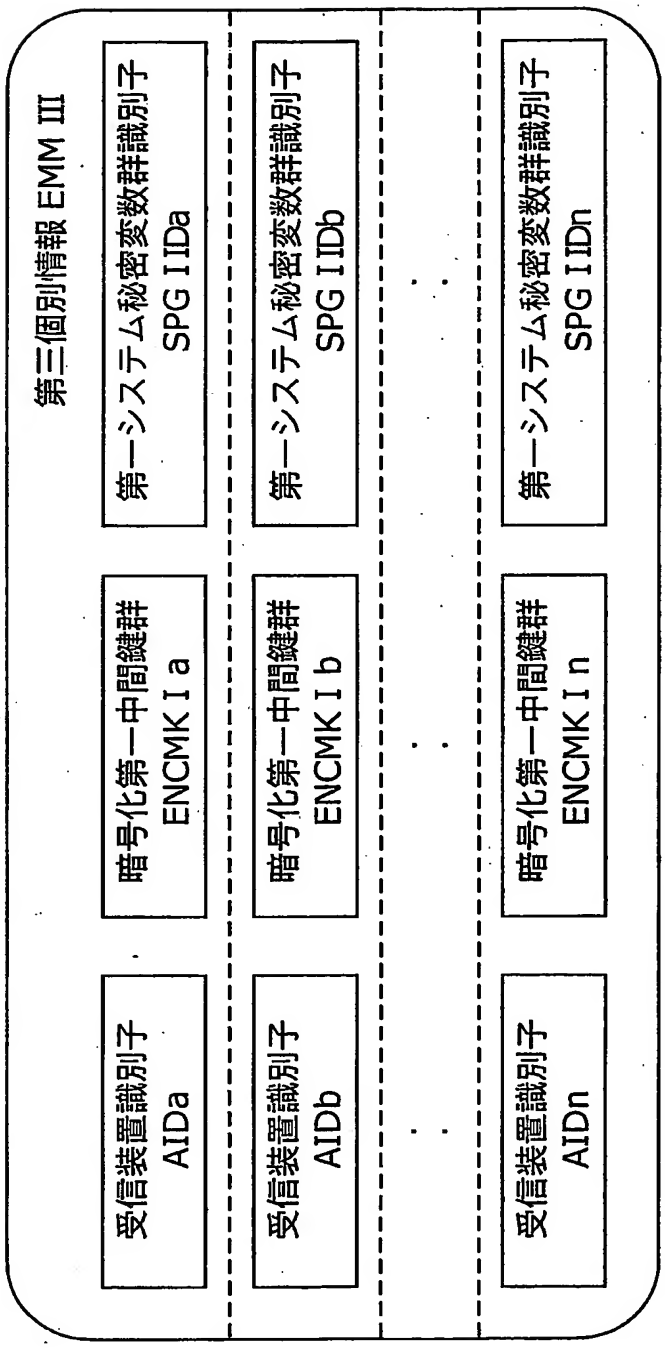
【図36】


114
受信装置対応情報
格納部
212
第三個別情報生成部
2122
第一中間鍵群
生成部
2121
第三システム
秘密変数数群生成部
第三システム
秘密変数数群集合
SPG III S
第三個別情報
EMM III
第三システム
秘密変数数群集合
SPG III S
第三個別情報
生成要求
REQEMM III

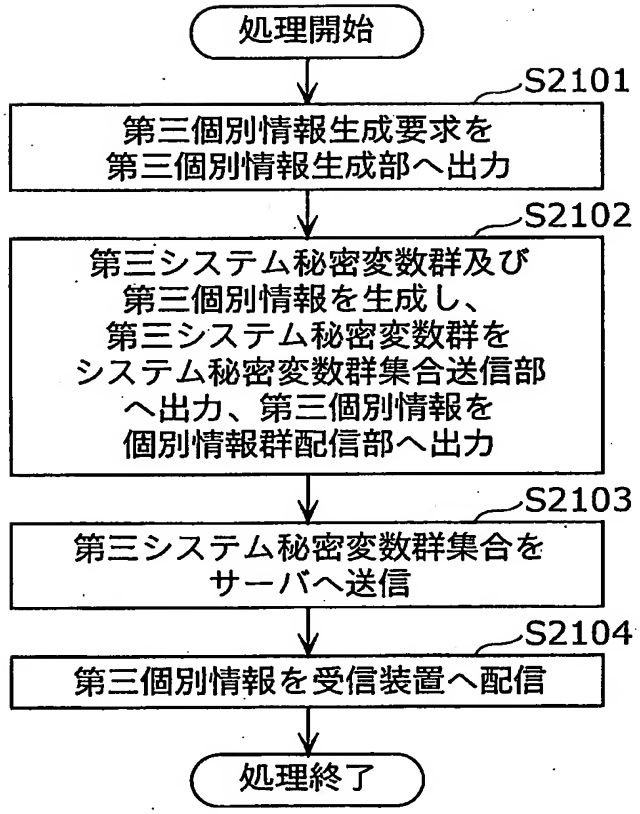
【図37】


第三システム秘密鍵群集合 SPG III S
第一システム秘密変数群識別子 SPG I ID 1
第一システム秘密変数群 SPG I 1
第一システム秘密変数群識別子 SPG I ID 2
第一システム秘密変数群 SPG I 2
第一システム秘密変数群識別子 SPG I ID 3
第一システム秘密変数群 SPG I 3
第一システム秘密変数群識別子 SPG I ID 4
第一システム秘密変数群 SPG I 4
第一システム秘密変数群識別子 SPG I ID 5
第一システム秘密変数群 SPG I 5
第一システム秘密変数群識別子 SPG I ID 6
第一システム秘密変数群 SPG I 6

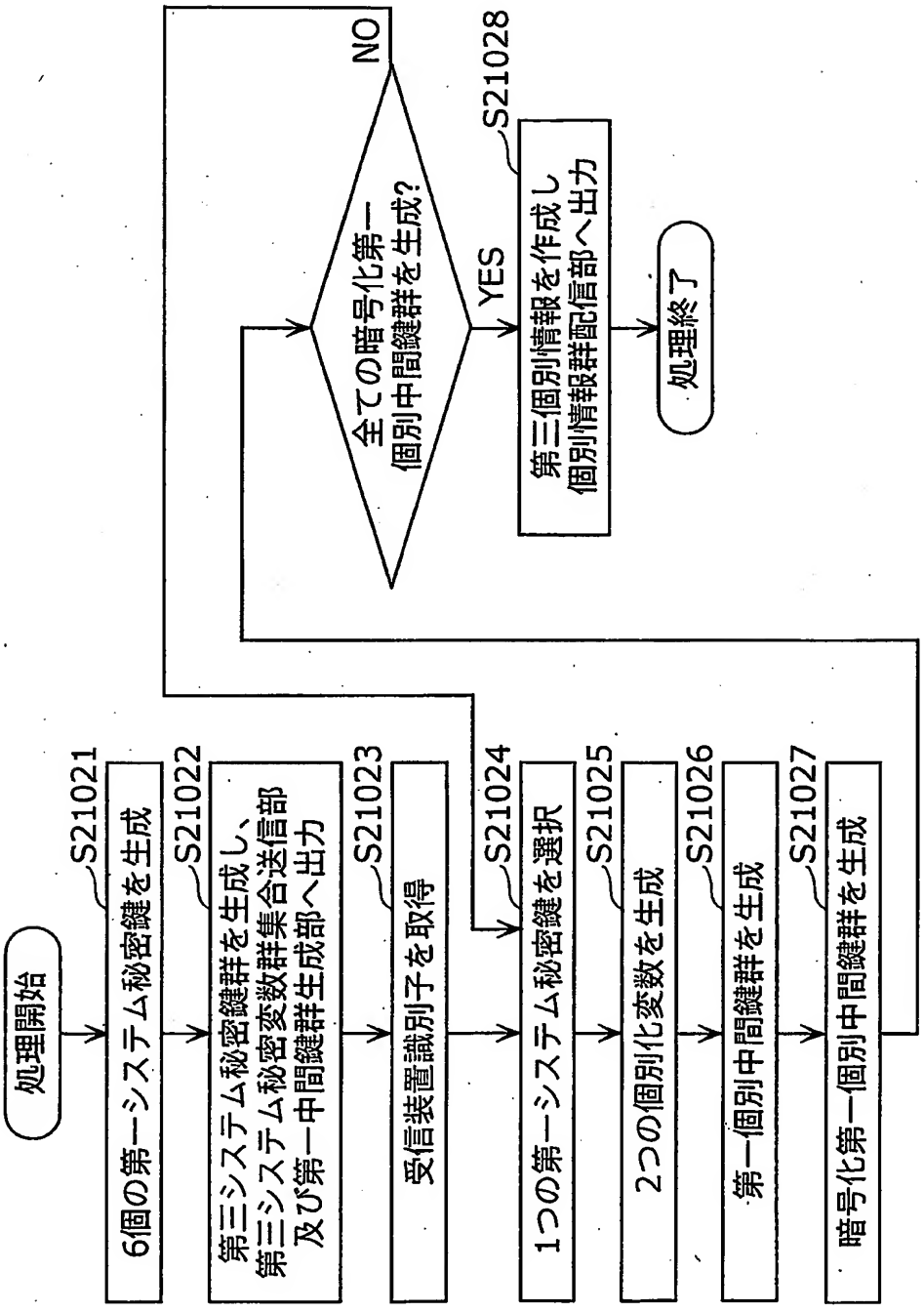
【図38】


第三個別情報 EMM III
第一システム秘密変数群識別子 SPG I IDa
暗号化第一中間鍵群 ENCMK I a
受信装置識別子 AIDa
第一システム秘密変数群識別子 SPG I IDb
暗号化第一中間鍵群 ENCMK I b
受信装置識別子 AIDb
第一システム秘密変数群識別子 SPG I IDn
暗号化第一中間鍵群 ENCMK I n
受信装置識別子 AIDn

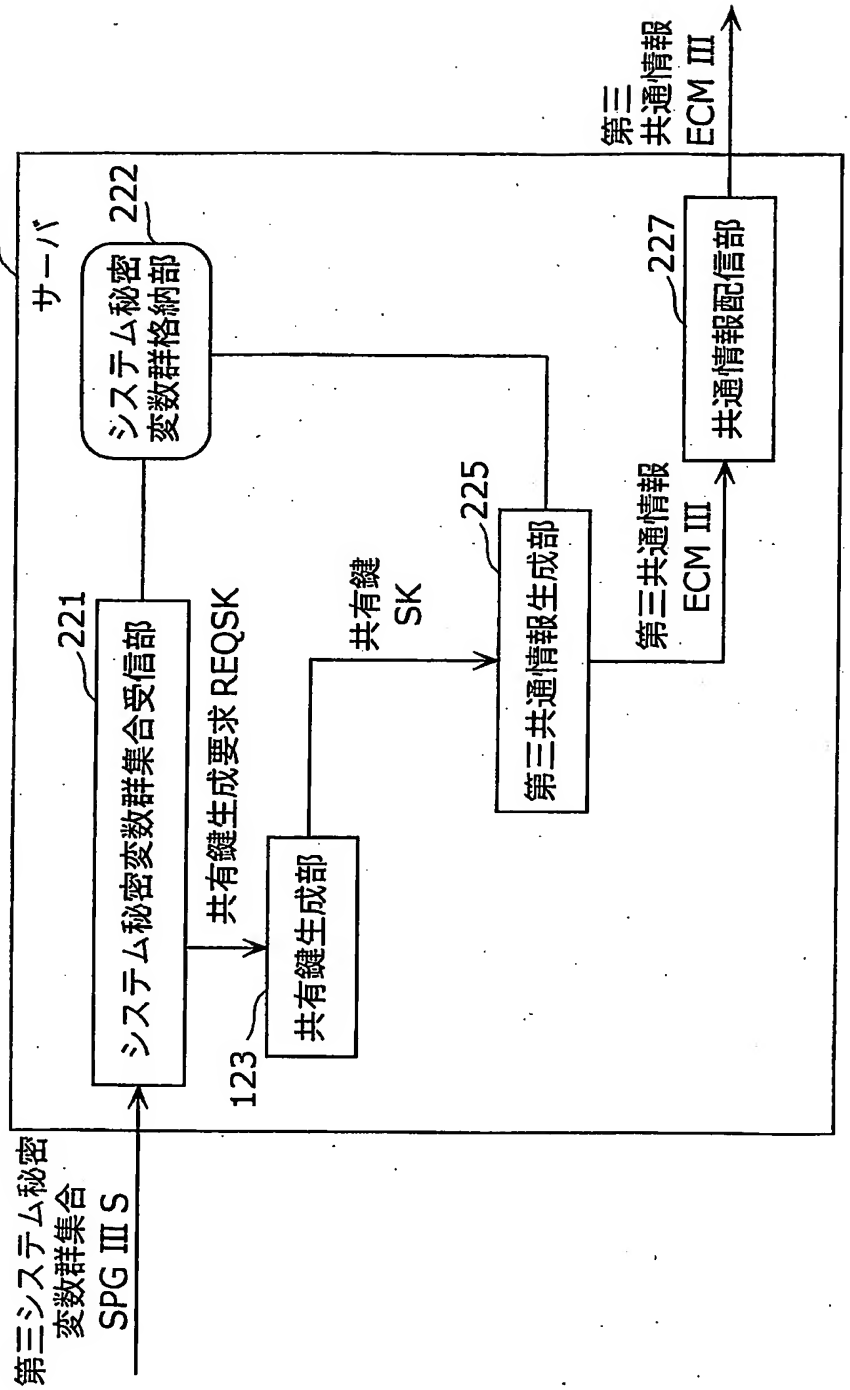
【図39】



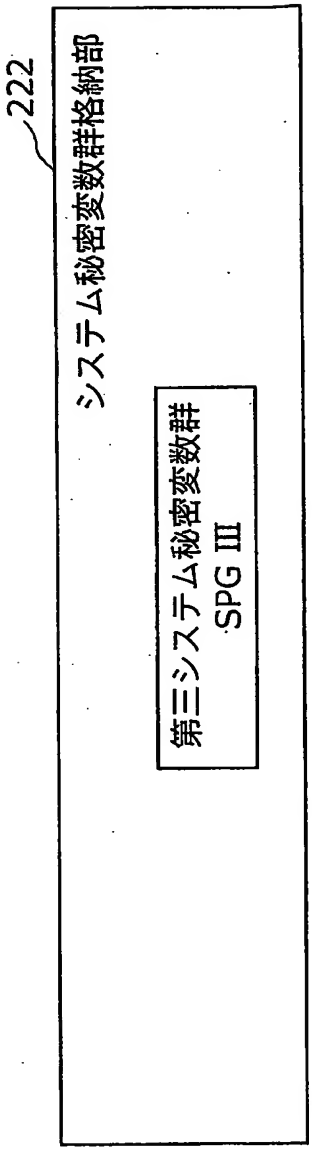
【図40】


処理開始
S21021
6個の第一システム秘密鍵を生成
S21022
第三システム秘密鍵群を生成し、
第三システム秘密変数群集合送信部
及び第一中間鍵群生成部へ出力
S21023
受信装置識別子を取得
S21024
1つの第一システム秘密鍵を選択
S21025
2つの個別化変数を生成
S21026
第一個別中間鍵群を生成
S21027
暗号化第一個別中間鍵群を生成
全ての暗号化第一
個別中間鍵群を生成?
NO
YES
S21028
第三個別情報を作成し
個別情報群配信部へ出力
処理終了

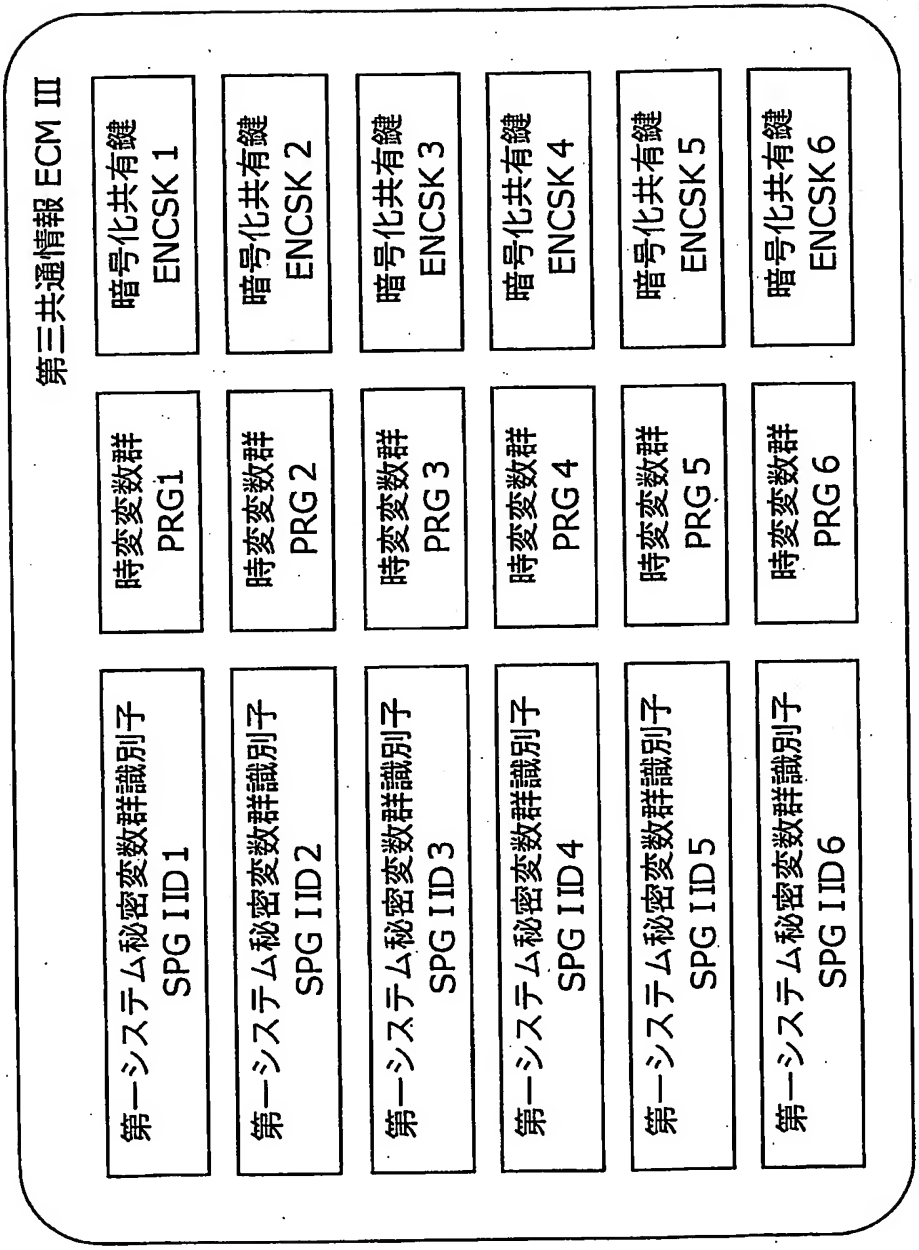
【図41】


第三システム秘密
変数群集合
SPG III S
22
サーバ
221
システム秘密変数群集合受信部
222
システム秘密
変数群格納部
123
共有鍵生成部
共有鍵生成要求 REQSK
共有鍵
SK
225
第三共通情報生成部
227
共通情報配信部
第三共通情報
ECM III
第三
共通情報
ECM III

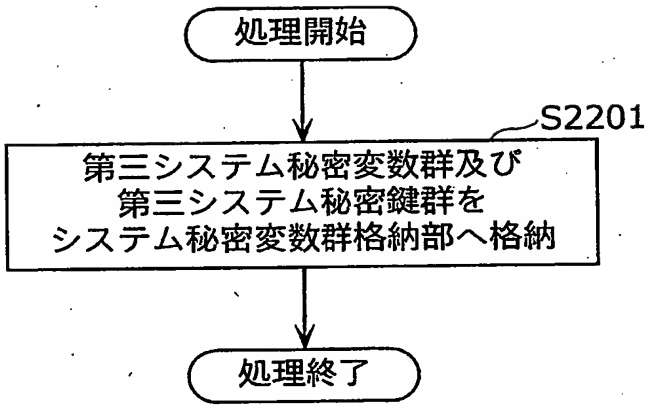
【図42】



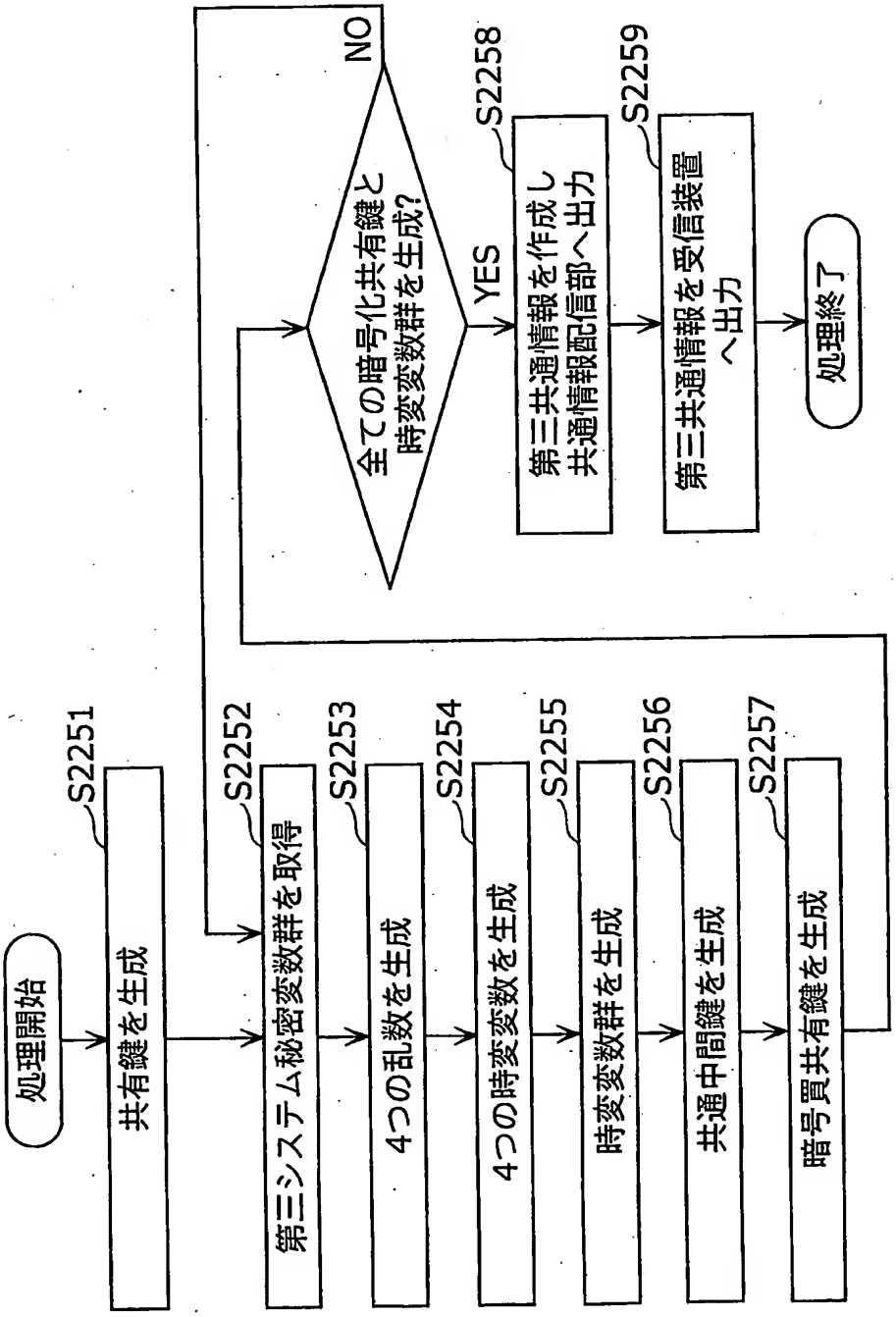
【図43】


第三共通情報 ECM III
第一システム秘密変数群識別子 SPG IID1
時変変数群 PRG1
暗号化共有鍵 ENCSK 1
第一システム秘密変数群識別子 SPG IID2
時変変数群 PRG 2
暗号化共有鍵 ENCSK 2
第一システム秘密変数群識別子 SPG IID3
時変変数群 PRG 3
暗号化共有鍵 ENCSK 3
第一システム秘密変数群識別子 SPG IID4
時変変数群 PRG 4
暗号化共有鍵 ENCSK 4
第一システム秘密変数群識別子 SPG IID5
時変変数群 PRG 5
暗号化共有鍵 ENCSK 5
第一システム秘密変数群識別子 SPG IID6
時変変数群 PRG 6
暗号化共有鍵 ENCSK 6

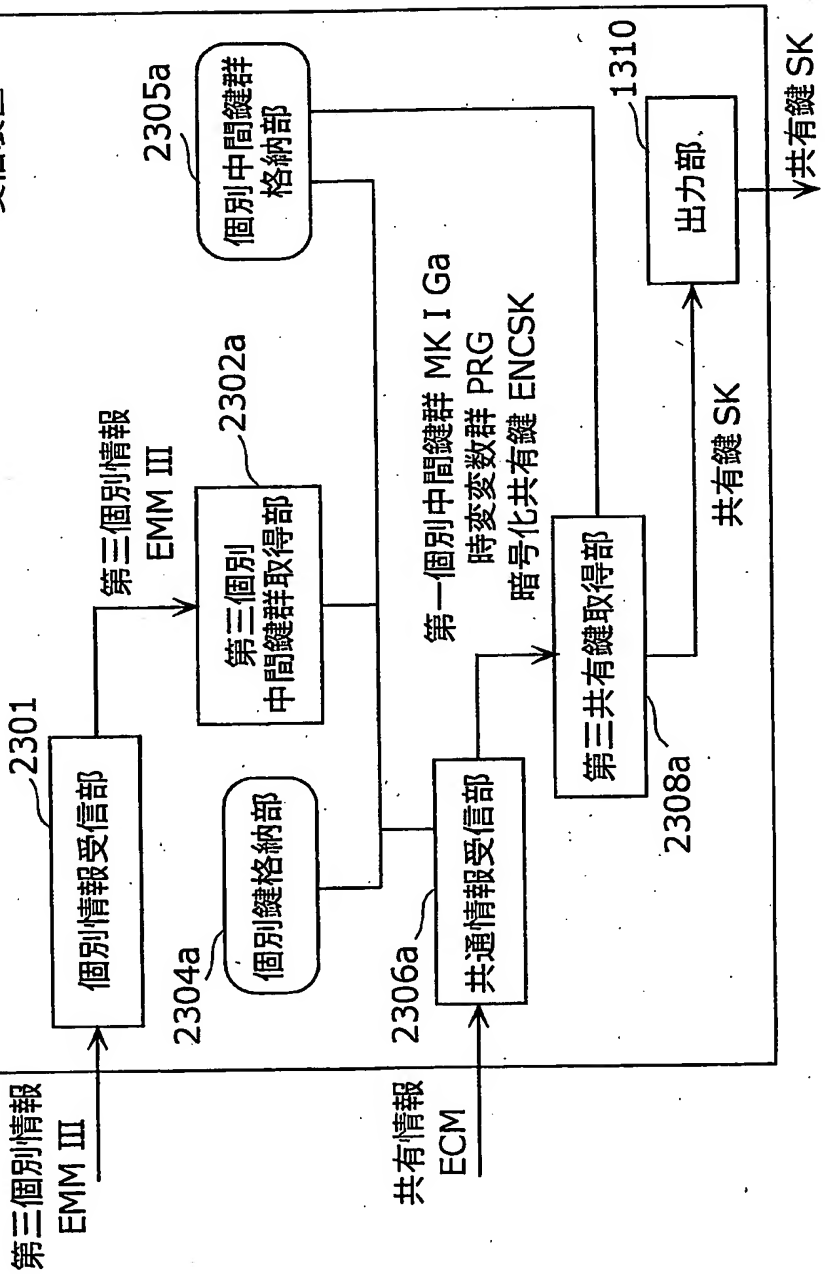
【図44】


処理開始
S2201
第三システム秘密変数群及び
第三システム秘密鍵群を
システム秘密変数群格納部へ格納
処理終了

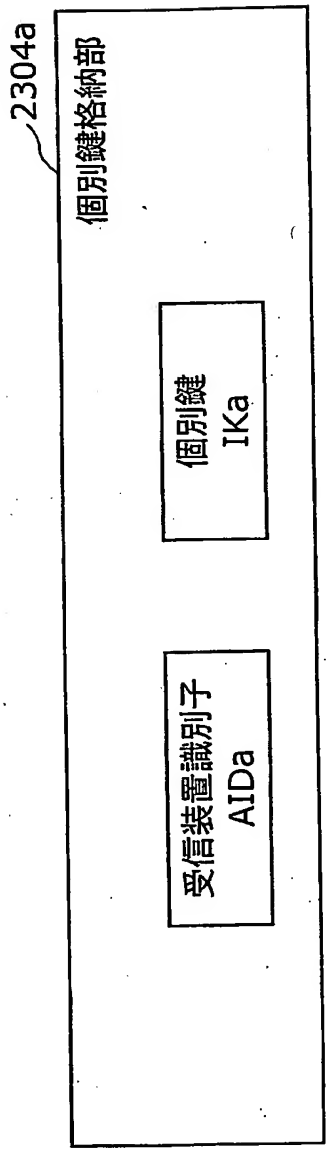
【図45】


処理開始
S2251
共有鍵を生成
S2252
第三システム秘密変数群を取得
S2253
4つの乱数を生成
S2254
4つの時変変数を生成
S2255
時変変数群を生成
S2256
共通中間鍵を生成
S2257
暗号買共有鍵を生成
全ての暗号化共有鍵と時変変数群を生成?
NO
YES
S2258
第三共通情報を作成し共通情報配信部へ出力
S2259
第三共通情報を受信装置へ出力
処理終了

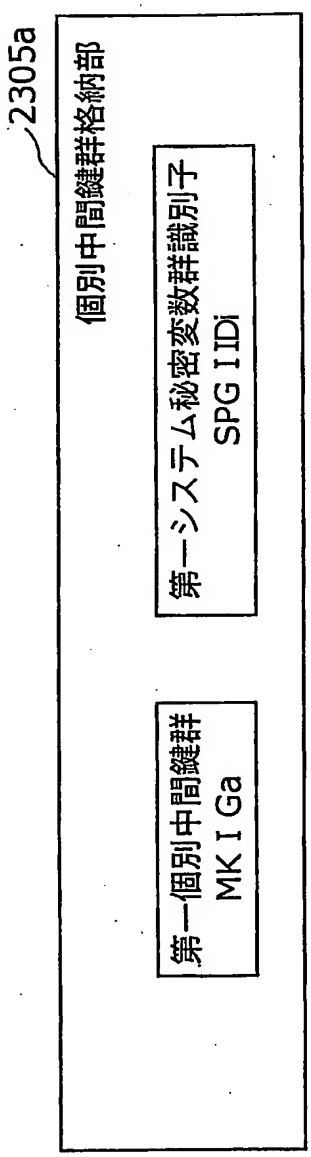
【図46】


23a
受信装置
2301
個別情報受信部
第三個別情報
EMM III
2302a
第三個別
中間鍵群取得部
2305a
個別中間鍵群
格納部
2304a
個別鍵格納部
2306a
共通情報受信部
第一個別中間鍵群 MK I Ga
時変変数群 PRG
暗号化共有鍵 ENCSK
第三共有鍵取得部
2308a
1310
出力部
共有鍵 SK
共有鍵 SK
第三個別情報
EMM III
共有情報
ECM

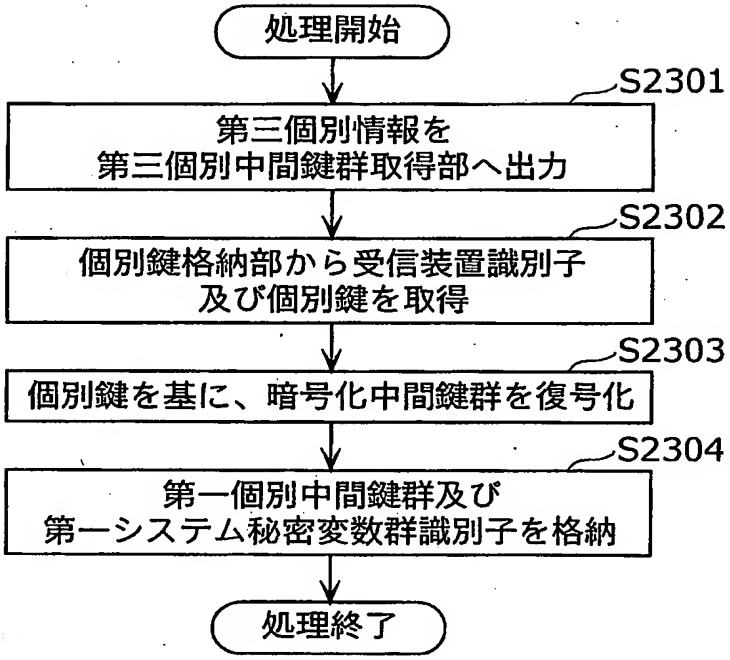
【図47】



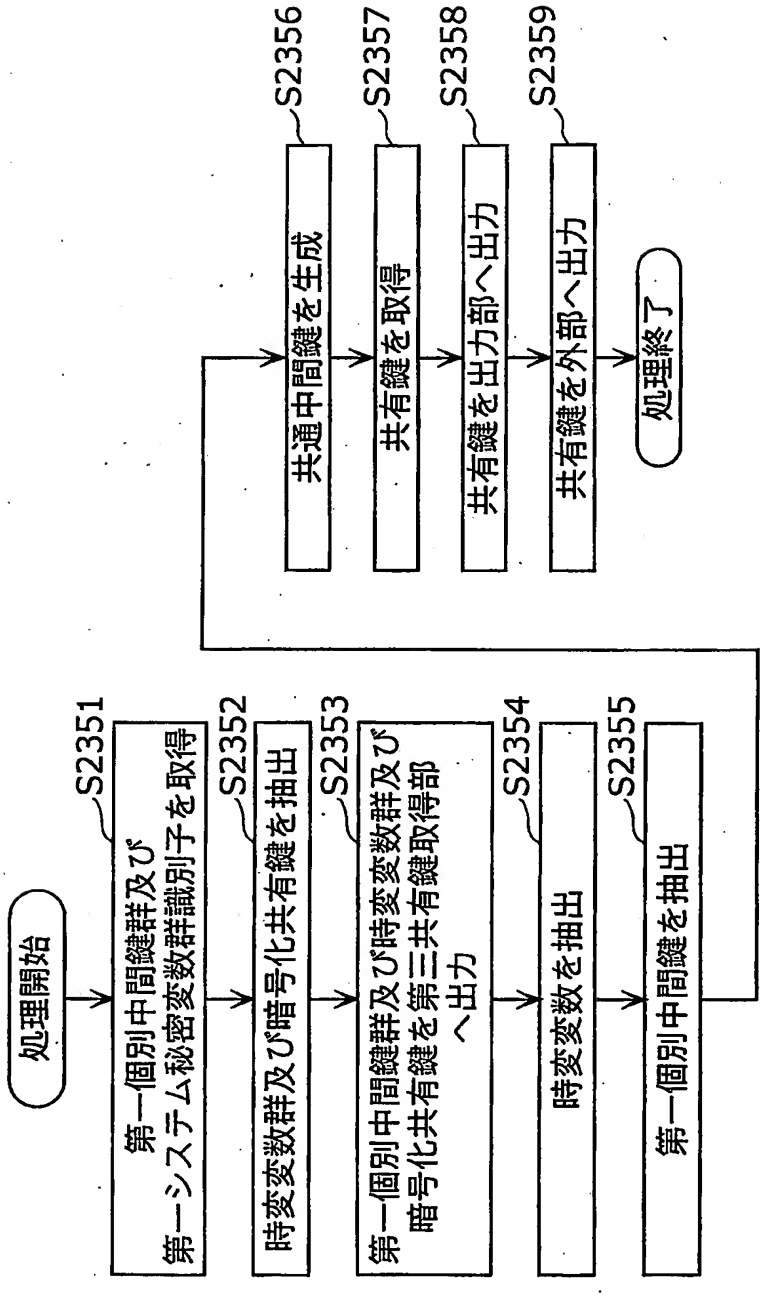
【図48】



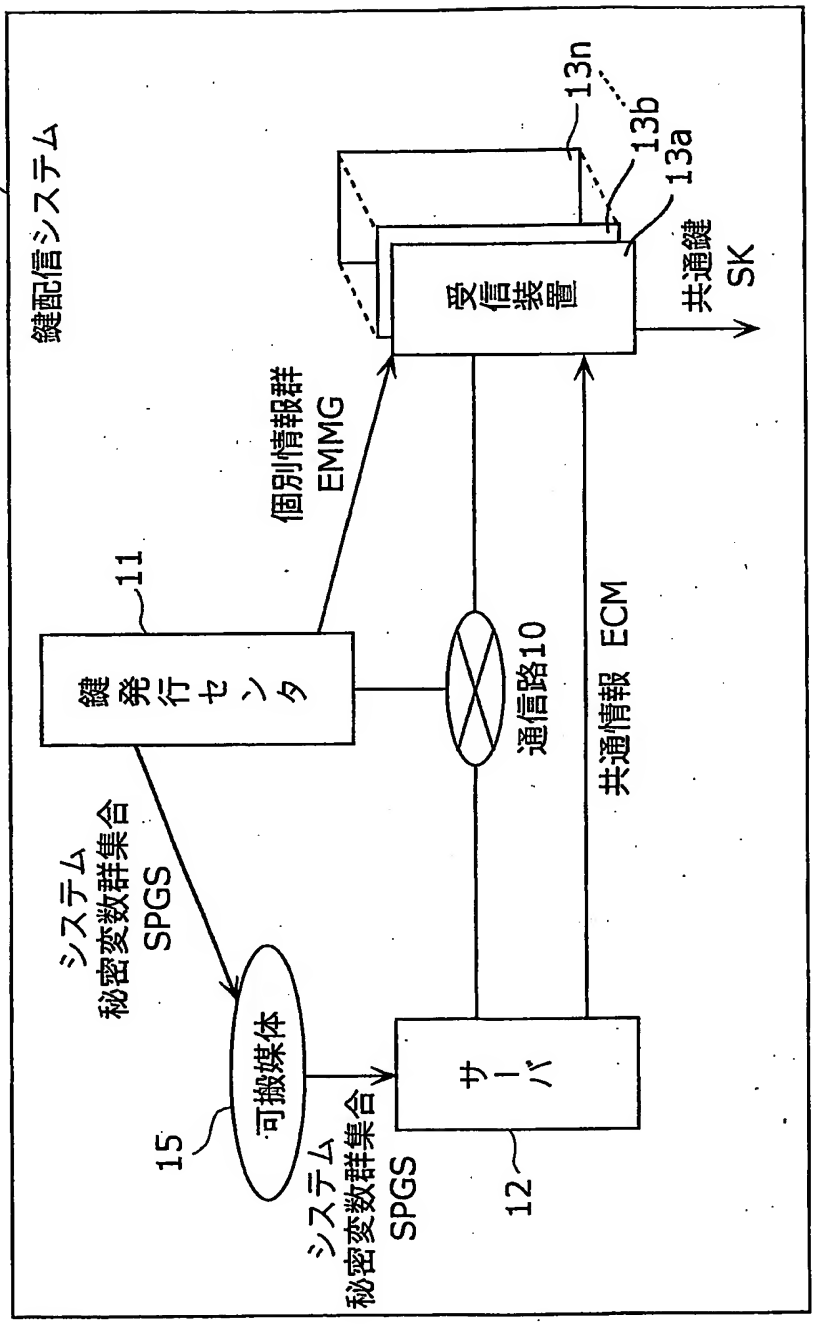
【図49】


処理開始
S2301
第三個別情報を
第三個別中間鍵群取得部へ出力
S2302
個別鍵格納部から受信装置識別子
及び個別鍵を取得
S2303
個別鍵を基に、暗号化中間鍵群を復号化
S2304
第一個別中間鍵群及び
第一システム秘密変数群識別子を格納
処理終了

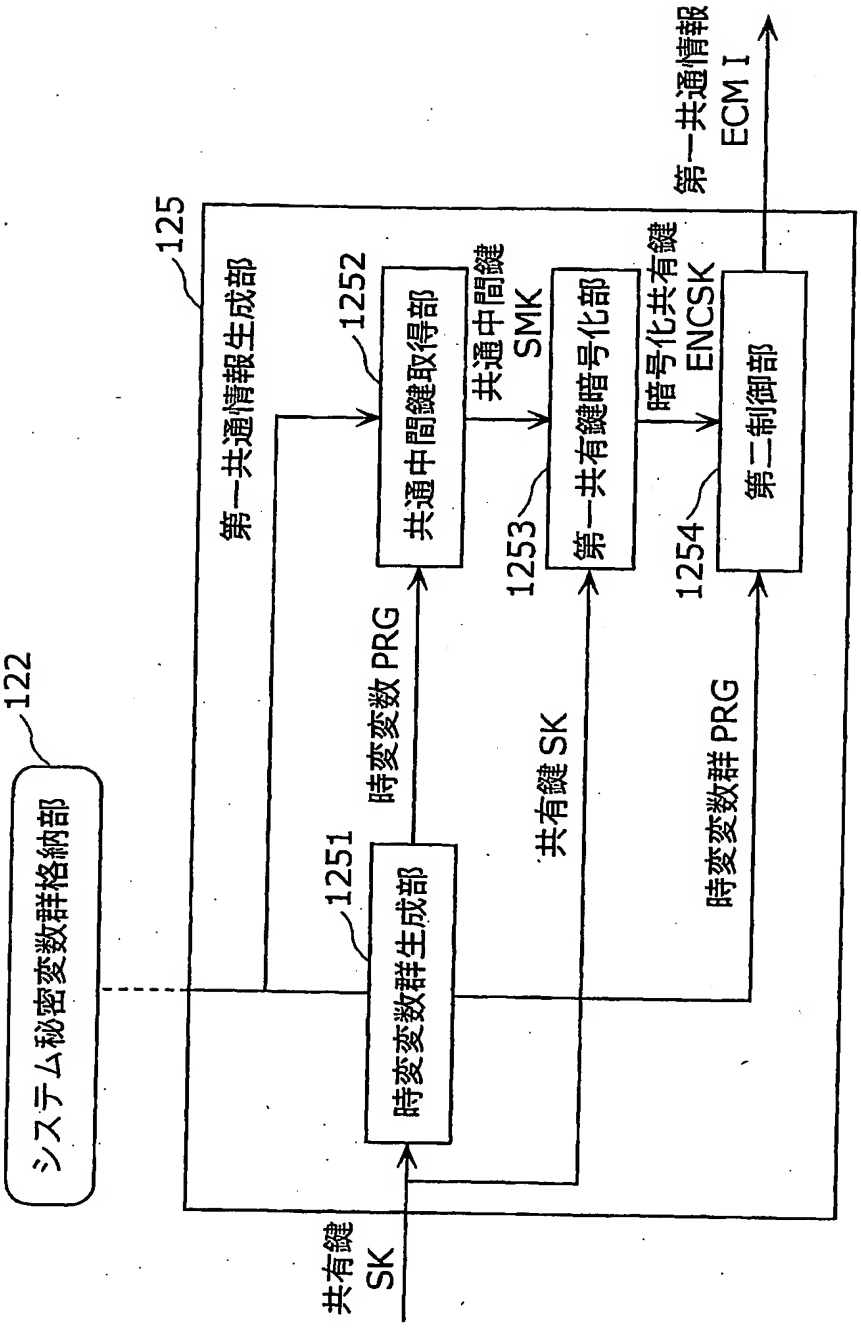
【図50】


処理開始
S2351
第一個別中間鍵群及び
第一システム秘密変数群識別子を取得
S2352
時変変数群及び暗号化共有鍵を抽出
S2353
第一個別中間鍵群及び時変変数群及び
暗号化共有鍵を第三共有鍵取得部
へ出力
S2354
時変変数を抽出
S2355
第一個別中間鍵を抽出
S2356
共通中間鍵を生成
S2357
共有鍵を取得
S2358
共有鍵を出力部へ出力
S2359
共有鍵を外部へ出力
処理終了

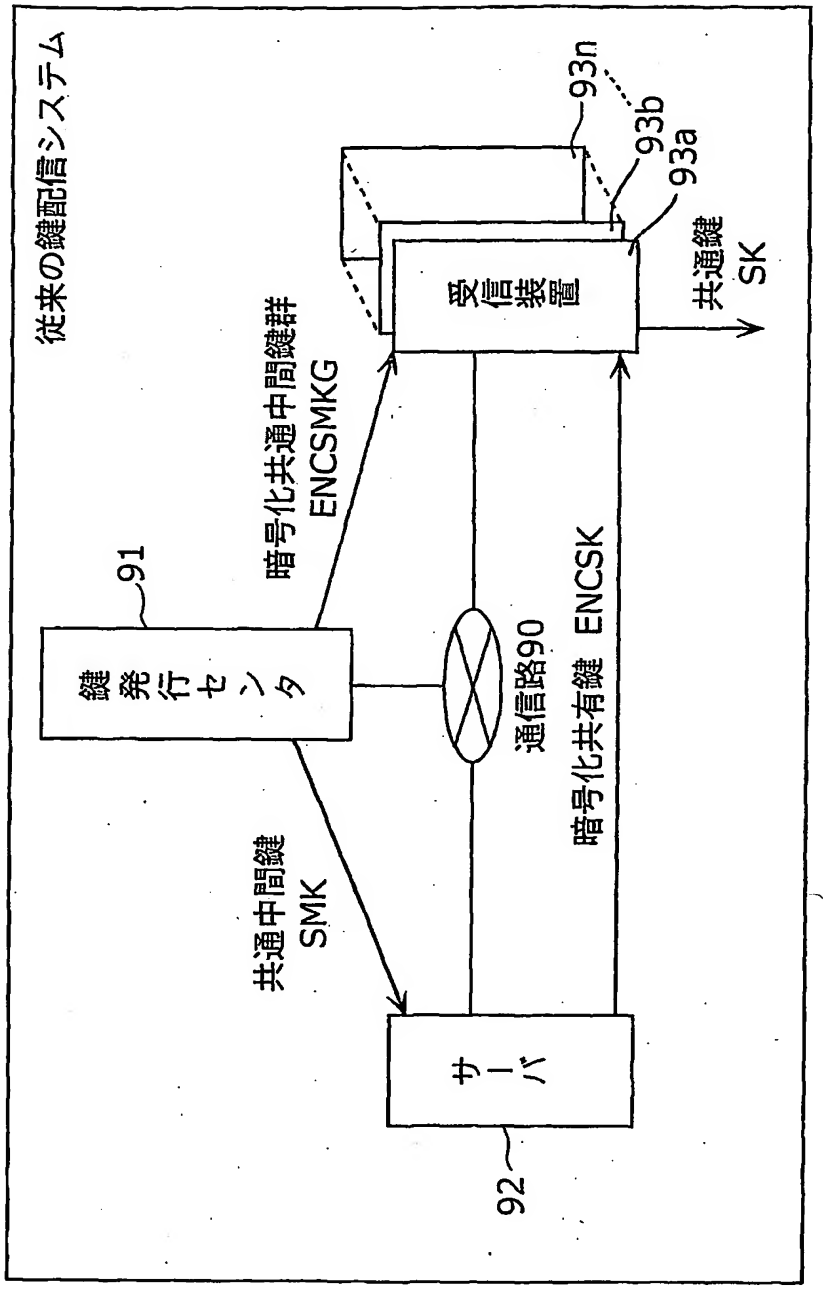
【図51】


1
鍵配信システム
13n
13b
13a
受信装置
共通鍵
SK
個別情報群
EMMG
11
鍵発行センタ
通信路10
共通情報 ECM
システム
秘密変数群集合
SPGS
可搬媒体
15
サーバ
12
システム
秘密変数群集合
SPGS

【図52】


125
第一共通情報生成部
1252
共通中間鍵取得部
共通中間鍵
SMK
1253
第一共有鍵暗号化部
暗号化共有鍵
ENCSK
1254
第二制御部
第一共通情報
ECM I
122
システム秘密変数群格納部
1251
時変変数群生成部
時変変数 PRG
共有鍵 SK
時変変数群 PRG
共有鍵
SK

【図53】



差替え用紙(規則26)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001359

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-313055 A (Hitachi, Ltd.), 09 November, 1999 (09.11.99), Full text; Fig. 6 (Family: none)	1-36
Y	JP 3-239033 A (Sony Corp.), 24 October, 1991 (24.10.91), Page 5, lower left column, lines 7 to 15; Fig. 1 (Family: none)	1-36
Y	JP 2-291740 A (Fujitsu Ltd.), 03 December, 1990 (03.12.90), Page 3, upper right column, line 6 to page 4, upper right column, line 20; Fig. 1 (Family: none)	6-12,22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 March, 2005 (11.03.05)	29 March, 2005 (29.03.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)